2013-03

NMCI TO NGEN: MANAGING THE TRANSITION OF NAVY INFORMATION TECHNOLOGY INFRASTRUCTURE

Chukwuelue, Chukwudi N.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/32806

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

NMCI TO NGEN: MANAGING THE TRANSITION OF NAVY INFORMATION TECHNOLOGY INFRASTRUCTURE

by

Chukwudi N. Chukwuelue

March 2013

Thesis Advisor:	Frank Barrett
Second Reader:	Mark Nissen

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE NMCI TO NGEN: MANAGING THE TRANSITION OF NAVY INFORMATION TECHNOLOGY INFRASTRUCTURE	**5. FUNDING NUMBERS**
6. AUTHOR(S) Chukwudi N. Chukwuelue	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The Navy and Marine Corps Intranet (NMCI), which is second only to the Internet in size, was supposed to be a mechanism to transform and support the Navy and Marine Corps with an IT infrastructure that would move the Department of Navy into the 21st century of warfare. Its function was to enhance command and control initiatives of the Navy and Marine Corps by harnessing the power of an integrated network. The current state of NMCI, though marred by a decade filled with marginal successes and many setbacks, is very positive, boasting more than 700,000 users, and consisting of over 380,000 work stations in more than 3,000 locations dispersed over seven continents. In 2008, Department of Navy leadership decided to move on and embrace the Next Generation Enterprise Network (NGEN) guided by early transition activities (ETA) and continuity of services contract. The use of the ETAs was to successfully mitigate the risk while migrating services from a contractor-owned, contractor-operated model to one that gives the government increased command and control. The purpose of this research is to examine the effectiveness of ETA and concurrent contracts in mitigating the challenges of migrating from the NMCI environment.

14. SUBJECT TERMS Navy Marine Corp Intranet, Next Generation Enterprise Network, NMCI, NGEN, Transition, Change Management, Stakeholder Management	**15. NUMBER OF PAGES** 127
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

NMCI TO NGEN: MANAGING THE TRANSITION OF NAVY INFORMATION TECHNOLOGY INFRASTRUCTURE

Chukwudi N. Chukwuelue
Lieutenant, United States Navy
B.S. Mathematics, Morehouse College 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Chukwudi N. Chukwuelue

Approved by: Dr. Frank Barrett
Thesis Advisor

Dr. Mark Nissen
Second Reader

Dr. Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Navy and Marine Corps Intranet (NMCI), which is second only to the Internet in size, was supposed to be a mechanism to transform and support the Navy and Marine Corps with an IT infrastructure that would move the Department of Navy into the 21st century of warfare. Its function was to enhance command and control initiatives of the Navy and Marine Corps by harnessing the power of an integrated network. The current state of NMCI, though marred by a decade filled with marginal successes and many setbacks, is very positive, boasting more than 700,000 users, and consisting of over 380,000 work stations in more than 3,000 locations dispersed over seven continents. In 2008, Department of Navy leadership decided to move on and embrace the Next Generation Enterprise Network (NGEN) guided by early transition activities (ETA) and continuity of services contract. The use of the ETAs was to successfully mitigate the risk while migrating services from a contractor-owned, contractor-operated model to one that gives the government increased command and control. The purpose of this research is to examine the effectiveness of ETA and concurrent contracts in mitigating the challenges of migrating from the NMCI environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AoA	Analysis of Alternatives
BAN	Base Area Network
C2	Command and Control
CAPE	Cost Assessment and Program Evaluation
CCA	Clinger-Cohen Act
CDD	Capability Development Document
CDR	Critical Design Review
CI	Configuration Item
CIO	Chief Information Officer
CONOPS	Concept of Operations
CoSC	Continuity of Services
COTS	Commercial-Off-the-Shelf
CNO	Chief of Naval Operations
CPD	Capability Production Document
CPIC	Capital Planning and Investment Control
CTE	Critical Technology Elements
DAS	Defense Acquisition System
DCAA	Defense Contract Audit Agency
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DoD	Department of Defense
DoDD	Department of Defense Directive
DON	Department of the Navy
EDS	Electronic Data Systems
ELA	Enterprise License Agreements
ETA	Early Transition Activities
FAR	Federal Acquisition Regulations
FDDR	Full Deployment Decision Review

FOC	Full Operational Capability
GAO	Government Accountability Office
GFE	Government Furnished Equipment
GIG	Global Information Grid
GOCO	Government-Owned Contractor-Operated
GOGO	Government-Owned Government-Operated
HP	Hewlett-Packard
IA	Information Assurance
ICD	Initial Capabilities Document
IOC	Initial Operational Capability
IEEE	Institute of Electrical and Electronics Engineers
IPT	Integrated Product Team
ISOOA	Independent Security Operations Oversight and Assessment
IT	Information Technology
ITAM	Information Technology Asset Management
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
LAN	Local Area Network
LPTA	Lowest Price Technically Acceptable
MAGTF	Marine Air-Ground Task Force
MAIS	Major Automated Information System
MCEN	Marine Corps Enterprise Network
MCHS	Marine Corps Common Hardware Suite
MCNOSC	Marine Corps Network Operations and Security Command
MD	Management Domains
MDD	Materiel Development Decision
MITSC	MAGTF Information Technology Support Center
MOE	Measurements of Effectiveness
MSA	Materiel Solution Analysis
NGEN	Next Generation Enterprise Network

NMCI	Navy Marine Corps Intranet
NOC	Network Operation Centers
OMB	Office of Management and Budget
OPEVAL	Operational Evaluation
OSD	Office of the Secretary of Defense
OSD CAPE	Office of the Secretary of Defense Cost Assessment and Program Evaluation
PCS	Permanent Change of Station
PM	Program Manager
RFP	Request for Proposal
SACM	Service Asset and Configuration Management
SDS	System Design Specification
SLA	Service-Level Agreement
SOA	Service Oriented Architecture
SPO	System Program Office
SWOT	Strengths, Weaknesses, Opportunities and Threat
USD AT&L	Under Secretary of Defense Acquisition, Technology, and Logistics

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I thank God for his grace that was sufficient for me; I am nothing apart from him.

To my angel, Ruby, and my boys, Alexander and Christopher: You are the reason I keep pressing on. Thank you for all the love, patience, support and prayers.

To Dr. Barrett: Thank you for your patience, advice and friendship, and most of all, for saying “yes to the mess.”

To Chris G, Marvin, and Chris B: These two years have been awesome because of you. Thank you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. THESIS SUMMARY AND RESEARCH METHODOLOGY

A. INTRODUCTION

This chapter introduces the thesis topic, provides a brief overview of each chapter, and presents the thesis research methodology. This thesis seeks to assess Department of the Navy's implementation strategy by comparing the implementation of the Navy Marine Corps Intranet (NMCI) and the Next Generation Enterprise Network (NGEN). Second only to the Internet in size, NMCI was supposed to be a mechanism to support to the Navy and Marine Corps with an information technology (IT) infrastructure that would move the Department of the Navy (DON) into the 21st century of warfare. Its function is to enhance command and control initiatives of the Navy and Marine Corps by harnessing the power of an integrated network. The current state of NMCI is very positive despite its calamitous beginnings, as it boasts over 700,000 users and comprises over 380,000 work stations in more than 3,000 locations dispersed over seven continents. This robust network annually facilitates the transfer of over 3.5 terabytes of data, while denying in excess of two million unauthorized access attempts (DoD, 2009). The entire intranet is designed to have fail-safe security by operations stemming from four decentralized network-operating hubs. Amidst speculations of the need for change, the DON has decided to move to the Next Generation Enterprise Network. Reasons for change include a need for the government to have more control over the network, better information assurance, and an improved defense posture against looming cyber threats. This thesis will show how the Navy's leaders are not leveraging the lessons learned from the implementation of NMCI and will therefore make the same mistakes.

Chapter II gives an overview of the DON network enterprise starting with a brief history of NMCI, its current state, and its future state as NGEN. The third chapter provides a detailed analysis of the early transition activities (ETA), focusing on the effectiveness of the ETAs as they facilitate the transition from NMCI to NGEN, and their ability to provide the desired future state. The fourth chapter focuses on the common factors that lead to failures in implementing IT using the "Strengths, Weaknesses, Opportunities and Threats" (SWOT) model. The chapter will also provide in-depth stakeholder analyses before, during, and after the change, and recommend a robust change plan that will leverage existing ETAs and industry best practices in enhancing the transition process. The final chapter summarizes the work and provides recommendations for further work.

In addition to recommendations for enhancing the transition process of large and complex IT initiatives in the DoD, this thesis raises many questions for future research, such as how can the government operate NGEN with a combination of low price and high performance with a segmented network run by multiple contractors? With too many stakeholder relationships, can the government leverage the nine best practices associated with developing and maintaining a reliable schedule in the ongoing change process with NGEN? And, how can leaders, especially in large and complex organizations, resist or refuse to acknowledge realignment feedback that could help the process? Though this thesis does not overtly provide the answers to these questions, it offers opportunities for consideration that can help in the averting more costly implementations in the future.

B. CHAPTER SUMMARIES

1. Chapter II: History of NMCI

The “need” for the Department of Defense (DoD) to attain information superiority was led DoD and DON leadership to create a system that had the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same. These leaders felt the daily functions of DoD was becoming more reliant on information technology it was time to let go of the current way of doing business. The problem would turn out to be not a system, but a prevalence of systems, disparate networks that handled several complex operations but were incapable of communicating with other systems.

The DON Chief Information Officer (CIO), established by the 1996 Clinger-Cohen Act, would be ill-equipped to deal with the vast number of unique IT systems, and in 1998 decided to establish a common network. The common network would be known as the Navy-Marine Corps Intranet and it would face incessant impediments, none of which would be more intense than that of the United States Congress. Congress’s source of contention was DON's attempt to bypass the usual process of issuing its request for proposals, a formal analysis of alternative program options and a business case analysis. Congress would eventually assume control of the NMCI procurement process and further choke the growth of the budding intranet.

Echelon II commanders also expressed resistance to the common network idea as the reality of it loomed closer. A variance in IT funding was a stumbling block for some Echelon II commanders especially those commands that had access to more funds than others. These opulent commands resisted the notion of parity and eventually received the attention of the civilian leadership and an order of forced compliance.

Electronic Data Systems (EDS) eventually won the contract. The next step was the daunting task of consolidating over 200 different computer networks and linking over 400,000 desktop computers that were dispersed throughout Navy and Marine Corps commands. The environment and the task were particularly disconcerting to EDS because each command encompassed thousands of personalized storehouses with a variety of customized hardware and software that was incompatible with NMCI's security protocols.

The unsettling environment impeded overall implementation and increased over time, causing catastrophic financial losses for EDS. As of mid-2000, the Navy still had over 1,000 legacy networks or devices that were running about 11,000 applications. This unexpected number of legacy systems led to schedule delays and cost overruns. After many years of contending with and trying to appease Congress, EDS and the end-user, DON, saw NMCI revitalize.

As NMCI continued to gain traction, the pressure from Congress started to wane, and with the change of Congress's leadership and amidst incessant negativity, DON again contemplated the standards and requirements for an information technology network to succeed the multibillion-dollar NMCI after the contract expired. DON now saw the prudence in diligently researching, clarifying, and aligning the relationships between IT requirements and the acquisition community so as to best be able to respond efficiently to direction from higher authorities. The progeny of the alignment of IT requirements and the acquisition community would be a successor of NMCI, the Next

Generation Enterprise Network. DON planned an incremental implementation of NGEN to avoid disrupting service to any exiting capabilities, and it had to be in place before the NMCI contract ended. Like NMCI, the procurement of NGEN would be novel as DON developed an acquisition strategy that allowed for several options and combinations of contracts that could easily be adjusted to meet current and future environments.

2. Chapter III: Early Transition Activities and Contracts

This chapter highlights the ETA and follow-on contracts to give an in-depth description of what they are and their intended purpose. This chapter also evaluates the effectiveness of the ETA and the overall transition from the NMCI environment to the NGEN environment.

In 2009, DON officials, leveraging lessons learned from the NMCI transition, began to develop ETAs to prepare for a successful migration of services from a contractor-owned contractor-operated model to one that gives the government increased command and control. With the ETAs, DON officials plan to mitigate the risk of migration to the NGEN segmentation service model for both industry and the government.

Each segment represents an allocation of IT services, functions, tools, and roles and responsibilities associated with end-to-end service delivery that will be provided by contractors or government sources fielded through multiple competitive awards. DON officials understand the segmentation of the network will create seams that must be managed effectively to ensure successful delivery and continuity of services. The two primary segments to be awarded are enterprise services and transport services and the remaining three segments are end user hardware; enterprise software licenses; and independent security operations, oversight and assessment support.

In response to DON’s ETA process, the Government Accountability Office (GAO) was directed by Congress to ensure that the DON had sufficiently analyzed alternative acquisition approaches and demonstrated that a reliable schedule and executable program was being used. GAO officials showed that the overall NGEN acquisition approach was not grounded in a reliable analysis of alternatives approach and had a poorly derived integrated master schedule which was responsible for the delays of key program documentation and gate review decisions.

DoD, DON and Office of the Secretary of Defense (OSD) officials refuted the findings in favor of prior decisions to keep the NGEN rollout on pace in spite of the apparent shortfalls and risks. These risks had been identified in the past and had materialized into critical issues that stagnated the transition efforts and added several billions to the estimated cost at completion.

3. Chapter IV: NGEN and NMCI the Common Ground

The last chapter of this thesis discusses the reasons that led to failures in implementing IT by comparing the implementation process of NMCI and NGEN, and evaluating and addressing key weaknesses in the areas of stakeholder expectation, requirements development, and program management. Chapter IV was built using a variation of the SWOT model to show the many similarities between NMCI and NGEN implementation. The chapter highlights the erroneous strategies still being used for NGEN that were also used for NMCI, and recommends opportunities to ameliorate current deficiencies.

Of the many reasons that lead to failures in implementing IT, many experts agree that poor management, failure to meet stakeholders' expectations, and poor requirements development are amongst the top (Global IT project management survey, 2005*)*. Other failure causes include technology and technical issues, unpredictable external factors, and politically motivated requests embedded in the project; these obstacles make it difficult to manage and meet objectives. This chapter recommends holistic management practices that take into account the various stakeholders and the change process, and leverage key interdependencies. The intent is the application of a more robust model that aligns resources and activities, and provides means to identify critical paths, consequently providing a testable model applicable to all phases of IT change within the Department of Defense.

A disparity of expectations causes a challenge for the different stakeholder groups. The challenge is a result of the required negotiation and appeasement of all stakeholders with the intent of achieving a common ground to pursue the project goals and maintain the project management effort. The solution to the disparity in expectations is a shared vision because it ensures a buy-in to the idea for all parties concerned, and this vision (the desired state) comes alive only when it is shared. A dynamic relationship, rather than the unidirectional, command and control norm that is seen in the implementation of NGEN and NMCI, is the key to motivate people to coalesce and realize a desired vision.

In addition to a shared vision, there must be a meticulous requirements definition process that stems from a shared vision. If the requirements are not clearly stated up front, complexity is adversely affected and can exponentially increase the scope, cost, and time of the overall project. The solution to the problem of wasted funds on IT projects that have failed to deliver promised functionality is to build systems using an agile or modular development process (i.e., by breaking projects into more manageable chunks and demanding new functionality every few quarters).

Finally, failures in IT acquisition can be attributed to the high rate of personnel turnover in government acquisition and also a general lack of skilled personnel. The transient nature of DoD personnel is due to the frequent permanent changes of station (PCS) and the lack of skilled personnel can be attributed to the long-held misconception that IT detracts from war fighting. Though these issues pervade all areas of DoD, the solution offered is the active recruitment and retention of a competent cadre of program managers. Competent management is essential for each project because of the vast number of interdependent elements that vary and have to be identified and analyzed, a task that is not easily achieved even in the simplest of projects. These interdependencies can cause overt or covert disruptions that if not checked can cause major projects to fail.

C. RESEARCH METHODOLOGY

The research strategy for this thesis started with parsing significant facts from NMCI’s historical timeline to develop Chapter II and provide context for the comparison in subsequent chapters. The next step was to evaluate the NGEN requirements documents to fully capture current activities of the implementation process. This work was done concurrently with the review of technical manuals and other academic writings regarding change management and leadership, in order to compare the implementation processes of NMCI and NGEN.

The sources of data that contributed to the development of this thesis were mostly archival data, including news releases, Navy messages, NGEN program documents, GAO reports, and various publications and Internet websites.

D. CONCLUSION

The purpose of this chapter was to introduce the reader to this thesis's research topic, provide a broad overview of each chapter contained within this thesis, and provide the research methodology used to gather data. The next chapter will outline the entire history of NMCI beginning with the conception of a naval intranet and will end with the current state of NMCI as it transitions to NGEN. The history chapter provides a chronological account of NMCI to provide context and background information necessary to understand the complexities associated with large IT implementations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. HISTORY OF NMCI

Never before has it been more imperative for organizations to remain relevant to their stakeholders if they wish to survive, than in recent years. Organizations must not only execute core missions at a high level, they must always remain attuned to the internal (employee dissatisfaction, process incompatibility, etc.) and external (policy, economic trends and technological advances) needs for change (Anderson & Anderson, 2001). These requirements are true for any organization and more so for large and complex organizations where the difficulties of managing any transformation are greatly increased. Bridges (2009) identified the three phases of any transformation or transition as (1) the ending: letting go of the old ways and identity, (2) the neutral zone: when the old is gone and the new is not fully operational, and (3) the new beginning: when people develop the new identity, experience the new energy, and discover the new sense of purpose that make the change begin to work.

A. THE ENDING: LOSING AND LETTING GO

1. The Ending: The Genesis of NMCI

In the DoD, the need for change is often framed as a development process rooted in the articulation of higher-level policies, strategies, mission and objectives. The process starts with the generation of policy, which fuels strategies and missions, and during these missions military leadership makes various assessments. The focal point of the assessments is to evaluate and reveal performance and capability gaps between the status quo and a desired future state.

These needs are then vetted for legitimacy and approved if found deserving. The incumbent chairman of the Joint Chiefs of Staff General Shalikashvili expressed the “need” for DoD to attain information superiority in Joint Chiefs of Staff-issued Joint Vision 2010 (1997). He conveyed the urgency of establishing a system that had the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same; it was time to let go of the current way of doing business when it came to information technology.

The problem would turn out to be not a system, but an abundance of systems. At this point, virtually all of Echelon II[1] and III[2] commands had an in-house IT support staff that provided autonomous budgeting and management of customized IT systems. The entire DoD "enterprise" was made up of a vast number of disparate networks that handled several complex operations but were incapable of communicating with other systems. In GAO report (1998a), the office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD (C3I)) identified the enormous complexity and consequent failures that the disparate systems could pose. ASD (C3I) believed that the disparate nature of the networks had undermined all DoD's attempts at management and this difficulty continued to increase due to the proliferation of more unprotected and disparate networks. These networks had multiple gateways with virtually unhindered access for malicious intruders and, because of the decentralized nature of the networks, it was impossible to accurately assess the operational readiness of the networks' information systems and identify their information assurance requirements.

The autonomous and complex systems continued to pervade in the DoD in spite of the Clinger-Cohen Act (CCA), which was enacted in 1996 to reform acquisition laws and revamp the ailing management of information technology in the federal government. CCA (1996) established a CIO for each federal agency, an action that consequently led to the formation of the Chief Information Officers Council. The CIO was responsible for monitoring the implementation of IT standards (consistent with federal information technology architectures) to include common standards for interconnectivity and interoperability, categorization of government electronic information, and computer system efficiency and security. The CIO office promulgated the guidelines for its agencies' IT systems, but did not have much oversight concerning budget or the ability to enforce standards.

The DON CIO established by the CCA was ill equipped to deal with all of the Navy's 29 Echelon II commands, all of which exercised virtual autonomy in acquiring

[1] The Naval entities that report directly to the Chief of Naval Operations, including the Naval Air Systems Command, Office of Navy Intelligence, and Space and Naval Warfare Systems Command. Major Commands include entities that report directly to the Marine Corps, including Marine Forces Atlantic, Marine Forces Pacific and Marine Forces Reserve.

[2] Subordinate command to an Echelon II command

and managing their IT systems. Discretion on the purchase of IT-related components was done under the purview of what the command leaders deemed necessary and how much money was available at the end of each month. IT systems grew and morphed based on the "DNA" of their organic command; each network was an extension of the command culture. As these disparate systems continued to thrive, the lack of interoperability as well as deficiencies in network security became more apparent. The lack of standardization was no more apparent than when there was an influx of new personnel to a command. In the DON, frequent changes in duty stations and assignments are the norm, so personnel were often faced with unfamiliar operating systems, and associated software such as email e-mail. The transient nature of personnel impacted productivity throughout the Navy because of the lack of standardization of applications. The diversity and uniqueness of these systems further impeded the efforts of Navy and DoD officials to obtain visibility on how much was being spent and how to improve management and security. With enumerable unprotected gateways, intruders had many opportunities to exploit Navy networks and, in 2001, the number of intrusions experienced was estimated at over 16,000 (Munns, 2003).

In an effort to address the myriad of concerns with the networks within the DON, in 1998, the leadership of the Navy and the Marine Corps decided to establish single networks within the services. The Navy would develop the Navy Wide Intranet and the Marines, the Marine Corps Enterprise Network. Plagued with many disparate IT systems and many with duplicated efforts, the secretary of the Navy directed the seemingly incapable DON CIO to synergize the Navy and Marine efforts and to establish a common network that addressed the lack of interoperability.

Despite the apparent advantages in the notion of a secure and interoperable common network, the impetus for the network was overwhelmingly financial, and in March 1999, the assistant secretary of the Navy, research, development & acquisition further directed the combined efforts to be bought as a service (Taylor, 2006). The assistant secretary's intent was to leverage the expertise and investment of the civilian industry rather than having the DON reinvest in the same areas. The DON decided that the requirements of the new common network could be procured efficiently through a single private-sector entity providing end-to-end IT capabilities as a service under a long-term commercial-type "seat management" contract. Navy officials initiated the performance-based contract for NMCI, in June 1999 with six months of market research (Jordan & Johnson, 2007). On December 23, 1999, the Navy released a request for proposals (RFP) for the intranet with the expectation of awarding a firm, fixed-price contract with performance incentives (GAO, 2000).

Typically a premier document issued early in the procurement of systems, the RFP is used to accurately define the current state of the system that requires altering or replacing. With this level of detail, a supplier is able to offer solutions that could address the requirement; the overarching intent is the minimization of abstraction during the procurement process. However, the RFP drafted by the Navy leadership had a high level of abstraction and did not provide potential bidders with an accurate picture of the existing infrastructure. Most commands could not produce the total number of computers or applications, or give an intelligible assessment of the budgets and security posture of their networks when requested by the office of the Chief of Naval Operations (CNO) (Perkins, 2005). The RFP was released late in 1999, and as the Navy leadership awaited responses from the commercial sector, they instructed all commanding officers and component commanders to ensure any and all existing IT contracts would expire within the year. All commands had to participate in the nascent network and all efforts to expedite a future transition to NMCI were necessary (Taylor, 2006).

2. Losing: The Initial Struggle

Opposition to change can vary with the degree of change implemented and the expectation of the process. Bridges (2009) believes that in the process of transition, resistance is in response more to what has to be "let go" than to "what" is changing, and can take the form of foot-dragging or sabotage (p. 16). The Navy leadership began to face myriads of opposition, all culminating in a massive resistance to the idea of the intranet. The resistance to NMCI was both internal and external to the DON, but none was more intense than that of the United States Congress. The resistance from the legislative branch all stemmed from the decision of Navy leadership to deviate from the established process of "rubbing shoulders" and pacification of necessary "gatekeepers" in the procurement of

NMCI. Navy leadership bypassed the usual process of issuing the request for proposals to and a formal analysis of alternative (AoA) program options and a business case analysis. DON also lacked a definitive plan on how a project will be funded and all risk mitigation efforts intended to address significant risks associated with such large undertakings. Navy officials argued that since NMCI was being procured as service, Regulation 5000.2-R did not apply to the intranet effort. The regulation defines a Major Automated Information System as an automated information system acquisition program that requires total lifecycle costs in excess of $360 million in fiscal year 1996 constant dollars (GAO, 2000).

a. Congress

The procurement of NMCI using the utility model for buying IT capability on a per seat basis was a new concept that appeared to circumvent congressional committees' usual oversight power for reviewing, authorizing and appropriating funds for acquisition programs (Perkins, 2005). Navy leaders knew that the cost of NMCI would be several billion dollars, but they were confident that the intranet, when finished, would be a less costly IT infrastructure and that it would enable substantial future savings. Navy officials had hoped that the financing of NMCI could be handled by reprogramming and transferring funding that was already designated for IT services, thereby bypassing a lengthy congressional process, which would invite scrutiny from Congress on a micro level, with its members requesting a delay in the acquisition and implementation of the intranet until it was fully developed. Congress demanded to be included in the future budget request and given the proper level of congressional oversight (Taylor, 2006).

Congress challenged the idea of using funds already allocated to IT systems to fund the new intranet because there was no plan in place to address how the Navy intended to support the current legacy systems while trying to develop and implement a replacement. Additionally, the Navy had failed repeatedly to provide concrete financial accounts for current IT systems and expected savings that would justify the project.

Congress was also concerned with the circumvention of the Office of Management and Budget (OMB) Circular Number A-76. Circular A-76 outlined a mandatory process of cost benefit analysis of new outsourcing initiatives, and with NMCI, Navy leadership in essence would “alter” functions currently done by government employees without doing due diligence by comparing the outsourced cost with the lowest possible internal cost. As it stood, there was a potential and negative impact of NMCI implementation on employees of current naval networking and telecommunications systems. The Defense Information Systems Agency (DISA) was one of the organizations and was leading the opposition via Congress. DISA was responsible for providing and ensuring long distance communications to the armed forces. It argued that hundreds of jobs would be lost to the NMCI initiative and the imminent withdrawal of the Navy and the Marine Corps (which already has its own service-wide network) from the system would burden the Army and Air Force with excessive costs. The pace at which the Navy planned to build the intranet further raised doubt with Congress as to the Navy’s ability to properly structure and manage the huge NMCI contract. All the negatives associated with the innovative acquisition of the intranet would culminate in the idea of subversion from Navy leadership and the compulsion of Congress to take an aggressive stance.

Congress eventually took control of the NMCI procurement process and further choked the growth of the budding intranet. Congress insisted on the revision of the RFP to require that all bidders make provision to hire any displaced federal employees, and to create a small business set-aside program[3] for at least 35% of the work to go to small business subcontractors who otherwise might be elbowed aside by the giant umbrella contract (GAO, 2000). One of the additional requirements from Congress to the Navy leadership regarding NMCI was a mandate that the system go through an operational evaluation (OPEVAL). Though this requirement was a staple for most major systems acquisitions, it would prove to be a daunting task for the Navy. A typical OPEVAL is done on systems to verify that a proposed system meets all predefined

[3] Federal Government Goaling Program ensures that not less than 23% of all government contracts go to small businesses, not less than 5% to woman-owned small businesses, small disadvantaged businesses, and not less than 3% to service disabled veteran-owned small businesses and certified HUBZone small businesses.

operational requirements. The issue with the OPEVAL was that there had not been a system like the NMCI before, so all the operational requirements had to be drafted and defined for the first time. The OPEVAL process will continue for the next couple of years with an accretion in both requirements and complexity.

b. Echelon II Commanders

As early as 1997, Echelon II commanders had been involved in the inception of a central enterprise network and after two years of numerous and intense deliberations had reluctantly coalesced on the notion of a shared vision for an enterprise IT system (Perkins, 2005). This notional alliance would prove precarious as the reality of the network drew closer. As the RFP was being drafted, the office of the CNO tried to create an accurate picture of the state of the current disparate networks but was met with passive resistance. The Echelon II commands insisted that any data collected had to conceal the true amount that was being spent on IT. Perkins (2005) noted that commands went as far as refusal of automated methods to gather the information and this was met with little or no interference from the Echelon II commanders. The numbers produced from the lackluster inventory of the legacy applications would produce 22 thousand applications, which would prove to be only one-fifth of the total.

Some Echelon II commands had access to more funds than others. These commands had spent and continued to spend a significant amount of money on IT, buying the latest and the best that technology had to offer. At the other end of the spectrum were commands that bought IT services sparingly and had systems that consisted of antiquated servers and computers. The commands with IT opulence were most resistant to reporting accurate number of systems in their commands; an accurate report of all IT systems that included current financial expenditures would, in effect, decrease the overall funding to those commands if all funding used on current IT systems was diverted to fund NMCI. Though the new intranet would increase security and interoperability, it would also assure a level of parity in IT across the board and this meant that the days of unrestrained and lavish spending on IT would be gone. The stalling efforts of the commands would finally receive the attention of then secretary of the Navy, Honorable Richard Danzig. Feeling that he had given due diligence by listening to all concerns and tired of the passive objections from the commands, he ordered Charles Nemfakos, United States assistant secretary of the Navy (financial management and comptroller) to recapture all visible IT funding in the Echelon II budgets and redirect it to NMCI (Perkins, 2005).

The struggle internally from the commanders and externally from Congress would continue to plague the Navy leadership as they were confronted with an incessant balancing act of extracting data from reluctant commands and warding off the ever-growing restrictions from Congress.

3. Letting Go

With all transitions, there has to be some form of letting go of the old reality and the old identity of the status quo before change takes place (Bridges, 2009). Letting go for some stakeholders might be harder than for others, but this resistance has to be addressed for a successful transition.

The resistance continued and intensified, but NMCI survived its tumultuous beginnings, and, in October of 2000, a contract for the intranet in the amount of $6.9 billion was awarded to Electronic Data Systems Corp. EDS was selected to create a digital information network linking ships, bases, and service members around the globe. The nearly $7 billion contract would be meted out in increments with a five-year contract worth at least $4.1 billion and a three-year option worth at least $2.8 billion. The contract did not include a defined schedule for implementation because the Navy leadership believed the contract was based on compensation arrangements and payments tied to an “iron clad” service-level agreement (SLA) and user satisfaction. The leadership felt that the contract as drafted provided sufficient motivation for EDS to move as quickly as possible (Schneider, 2000).

EDS had earned the daunting task of consolidating over 200 separate computer networks and linking some 350,000 desktop computers dispersed throughout Navy and Marine Corps commands. With the largest federal IT contract ever competitively awarded, EDS, the main contractor, created a multidisciplinary team of companies known as the information strike force (ISF) to handle the overall project. The team included Raytheon (security), WorldCom (network connectivity) and General Dynamics (network consulting), as well as 200 subcontractors assembled to develop the new system that would be capable of putting huge resources at the fingertips of sailors and marines in the field. Some of the capabilities touted were the ability to conduct seamless and real-time troubleshooting between operational forces and appropriate resources; the myriad of possible issues that could arise could now be solved via face-to-face video conferencing or the accessing of databases from mobile devices at remote locations.

4. Leaving a Legacy

After the contract was signed, EDS and the Navy leadership were ready to begin the actual intranet implementation process. Congress wanted the process to be incremental and mandated that the initial rollout would be only 40,000 seats. After a successful test and evaluation period, DoD then could authorize installation of an additional 100,000 seats. The process for a site rollout involved EDS assuming acceptance of responsibility for a site and taking over the operation of the legacy network until the cutover to the NMCI environment. The environment that EDS came to face not only derailed the plan and schedule of the implementation, but also almost destroyed the entire process.

The environment was highly disconcerting to EDS because not only did it have to wait for DISA approval,[4] but each command was littered with thousands of computers (personal storehouses of everything from preferred screensavers and downloaded music to customized software) with applications that could not be installed on NMCI because they could not run on Windows 2000 or did not meet security protocols (Perkins, 2005). The end users in general appeared to be ill informed about what it would take to be part of the NMCI enterprise. This ignorance of the end user caused either apathy or blatant resistance. The apathy first manifested in benign but overt forms of frustration with the rigidity of the security levels or the complexity of the systems. The more adept user,

[4] The August 17, 2000 Memorandum of Agreement (MOA) required that DISA have the first opportunity to satisfy all wide area network (WAN) requirements and only in instances where DISA is not able to meet the service requirements. Commercial augmentation, i.e., EDS, would be allowed.

described as an end user with maximum control of a legacy system, would experience an unpleasant reality: the transition from a carte blanche localized control to a high degree of centralized control and operation. This more adept user exhibited an extreme form of resistance. In these extreme cases, actions often culminated in deliberate attempts to antagonize EDS's efforts during local installation. The ISF was required to determine the nature of all the legacy systems and vet the potential to migrate to the network, or scrap and replace. The process proved to be unusually arduous due to resistance from personnel and also because of the DoD information technology security certification and accreditation process.[5] As the certification process continued, the number of applications found at Navy commands continued to increase and the final number was estimated to exceed 100,000, with 30% of the number not being used (Perkins, 2005).

The difficulty of this environment was further compounded by the delays in constructing Network Operation Centers (NOC), which would serve as hubs of the new network. NOCs had to be built and put into operation before the process of cutover could be accomplished. Six had been planned initially, but the Navy leadership would settle on four based on recommendation from EDS (Taylor, 2006). NOCs were designed to provide around-the-clock network management and monitoring, user administration, and information security services to all seats on the NMCI network. The delay in construction of the NOCs added to the delays; however, the gross underestimation of the number of legacy systems proved to be the single point of impedance to the implementation efforts, and this setback sent ripples that soon were felt outside the confines of the Echelon II commands (Perkins, 2005).

One of the significant setbacks observed during the implementation at Quantico, VA, was that after the first 90 days of implementation, only 568 seats had been delivered, although the expectation had been the delivery of 30 seats a day (Jordan & Johnson, 2007). Lt. Gen. Edward Hanlon, then commanding general of the Marine Corps Combat Development Command, attributed the issues of implementation to an unprepared and under-resourced EDS team. The fact was that EDS had underbid significantly to win the

[5] The information technology security certification and accreditation process defines a process that standardizes all activities leading to a successful accreditation with the intent of minimizing the risks associated with nonstandard security implementations across shared defense information infrastructure and end systems.

contract and had invested nearly $2 billion of its funds into the system and was hemorrhaging millions of dollars; EDS recorded a loss of $316 million during the first six months of implementation (Jordan & Johnson, 2007). The increasing stagnation in overall implementation was directly proportional to the losses EDS would continue to endure. EDS's huge financial losses were partly due to inaccurate reporting, and in some cases no reporting, of the real impact of legacy systems, some of the systems being used for vital operations that could not be dispensed with. These legacy systems almost crippled the initial effort as more time than was allocated for the set-up of the infrastructure was used to either merge or migrate the legacy systems onto the NMCI infrastructure. Under the contract, EDS was guaranteed a minimum order per year and was only paid when a seat became operational. At that point, EDS was to be paid 85% of the contract seat price. After satisfactory execution of appropriate SLAs, then EDS could charge 100% of the seat price. Incentive payments were also contingent on end users' satisfaction as determined through on-line surveys conducted quarterly by an outside firm. At 85% satisfaction, EDS was scheduled to receive an additional $25 per seat; at 90%, $50; and at 95%, EDS would earn an additional $100 per seat (Perkins, 2005). The setbacks continued, and in the early stages of the network implementation, EDS posted a pre-tax loss of nearly $1 billion.

Congress interpreted the setbacks with NMCI as a failure of Navy leadership to appropriately curb the issues with the implementation. The response to this inefficiency was to release the Marine Corps from the program, excluding aviation depots and naval shipyards, and further reduce the amount requested by the president by $160 million (Taylor, 2006). Congress did not approve of the pace, testing methods, and the general handling of funding for NMCI. The leadership of the Navy, including the leadership from the Marine Corps, was very vocal about their opposition to the recommendations from Congress. They argued that the Marines were awaiting much needed refreshment that would be accomplished through the NMCI implementation. The accusatory tone from Congress countered by the vehement defense of the network and statements concerning funding from Navy leadership continued for months to come. The sentiment from Wall Street pundits was that EDS's cash flow problems were caused by the government's refusal to pay for EDS's NMCI work. In 2002, after much angst among the stakeholders, Congress extended the NMCI contract and mandated the Secretary of the Navy to name a single person "whose sole responsibility will be to direct and oversee the NMCI program" (Plummer, 2001). The Navy named Rear Admiral Charles "Chuck" Munns, a career submariner, to head the NMCI directors' office and a Marine Corps colonel, Robert Logan, as his deputy. The extension until 2010 brought the value of the contract to $8.82 billion (Onley, 2002).

B. THE NEUTRAL ZONE

1. Survival

The neutral zone, as described by Bridges (2009), is a period in the transition process when neither the old ways nor the new ways work satisfactorily. This was an appropriate description for NMCI as the number of applications that could not be installed continued to grow.

> As of January 2006, there was a 40% pass rate on the applications that have been re-tested for use on Windows XP. As extreme examples, the Naval Flight Planning System application (a popular flight planning program that allows pilots to calculate fuel consumption, print flight routes, and view satellite images of practice targets) and the Super Hornet squadrons' SAME maintenance application simply did not work on NMCI machines running the Windows XP operating system. Because of these and other incompatibility problems, NAS Lemoore has elected to stay with Windows 2000. (Taylor, 2006, p. 69)

NMCI continued to grow, albeit at a slower rate than expected, but with its slow accretion came a significant rise in overall DoD spending. This combination of slow implementation and a high price tag made NMCI a good candidate to get cut from the budget each year. In 2003, the House Armed Services Committee recommended across-the-board cuts of Pentagon information technology programs because of a lack of feedback on the programs' progress, and NMCI was top on the list. According to GAO report (2006) the intended pace projected between 412,000 and 416,000 seats operational by fiscal year 2004, but by August of 2002, EDS had assumed responsibility for operating and maintaining only 57,674 seats, 19,536 of which had reached "cutover." The project finally had the minimum numbers required by Congress to transition into the operational testing and evaluation assessments. The Navy was authorized to order an additional 150,000 seats, on top of the 160,000 that already had been authorized contingent upon successful testing and evaluation. Testing and evaluation of the network was marginally successful at some sites and a failure in others. For example, during

USMC Operational Analysis of the NMCI deployable solutions, the field operators could not access the NMCI help desk from deployed positions (DOT&E, 2003). Despite the results of the assessment, the Navy ordered the cutover of 150,000 seats, and the pace of deployment ramped up significantly; by mid-2003, 98,650 NMCI workstations had been brought online.

In 2003, with borderline improvements with the network implementation, NMCI was tested by the prevalence of viruses and worms that plagued many commercial and government networks. A series of major virus attacks, to include *Blaster*, *Nimbda*, *Iloveyou*, *SQE*, *Slammer* and *Sapphire*, running from 2002 to 2004, brought down or slowed vulnerable networks, but NMCI had successfully blocked 267 million attempted intrusions and detected 2,033 new viruses (Perkins, 2005). In August of 2003, NMCI lost the battle and succumbed to *Welchia worm*, which crippled service to thousands of computer users. Though the attack only affected the unclassified portion of NMCI, it affected more than 50,000 systems with a computer worm that slowed down or denied access to applications in the most severe disruption to ever hit NMCI. Recovery from the attack was a testament to the touted capabilities of NMCI, because after identifying the problem, Naval Network Warfare Command, with its subordinate Naval Network and Space Operations Command, together with NMCI prime contractor EDS, worked with anti-virus vendor Symantec and released a recovery patch within minutes of its availability across the entire centralized network (Ma, 2003a).

The network continued to survive and the pace of rollout improved to a rate of 1,000 NMCI workstations per day. Even with the improvement of rollout rate, the implementation was severely behind, with less than 145,000 stations vice the 350,000 stations expected by late 2003. The impedance to the process continued and was unique to each site. In one site, the seats could not be implemented because the schedule of implementation coincided with the deployment of Marines to Iraq. At some sites, asbestos in buildings slowed down the process because work had to stop while the harmful material was removed from the walls. Some sites presented peculiar forms of challenges, such as a site in Crane, IN, where an electric generator had to be added to support a server farm. To add the generator, the crew had to cut down some trees. But

Indiana brown bats, an endangered species, were nesting in those trees, and work had to stop until nesting season was over (Ma, 2003b).

2. NMCI Turns the Corner

NMCI continued to gain traction as the pressure from Congress started to wane and with the change of its leadership. In August of 2004, Rear Admiral James B. Godwin III succeeded Admiral Munns as the new director of the NMCI program office. As a former lead systems engineer and deputy program manager of the F/A-18 strike fighter program at the Naval Systems Command with experience as a program executive officer for tactical aircraft programs, Godwin brought with him practical and proven best business practices which he would apply to the NMCI project. The Navy would also restructure the NMCI program, moving oversight of all business IT, server consolidation, and legacy network reduction to a new program office headed up by Godwin. The move was designed to improve the effectiveness and efficiency of Navy IT acquisition (Onley, 2005). With Admiral Godwin came changes in the SLAs as the number was slashed from over 200 to 37. The original NMCI contract consisted of 44 SLAs with 192 performance categories. The original SLAs and performance categories for NMCI delineated specific performance characteristics that had to be met by EDS to avoid payment penalties. In some cases, the terms did not provide sufficient incentives to meet requirements. EDS leadership often opted to fail SLAs and suffer the 15% penalty instead of suffering a much larger expense to meet the SLA requirements. The reduction was to make the SLAs more focused on end results rather than on interim steps, and to make them more measurable.

The revised SLAs allowed the ailing EDS, which had reported negative cash flows in years 2001 through 2004 with a total of over $1 billion in losses, to eventually profit from the program and experience positive cash flows beginning in 2005 (Ma, 2004). With EDS edging ahead financially for the first time since winning the contract, it sought more than $780 million from the Navy for unanticipated costs for Pentagon IT reconstitution after Sept. 11, 2001, and the expenses associated with reducing legacy applications. Navy leadership only agreed to a fraction of the claim and offered $100 million to settle the contract dispute. In March of 2006, Navy leadership and EDS finally worked out their differences and with the $3.1 billion contract extension making EDS the sole provider and operator of the intranet until 2010. The impetus to resign EDS instead of letting the contract expire in 2007 was the ongoing global war on terrorism. NMCI had become a vital part of day-to-day naval operations and the leadership felt it vital to have uninterrupted connectivity for users (Taylor, 2006).

GAO report (2006) stated that about 303,000 seats were operational at about 550 sites by June of 2006. Navy leadership claimed the current delays of implementation were attributed to the certification and accreditation process for all applications, as well as the legislation requiring certain analyses to be completed before seat deployment could exceed specific levels. The report further claimed that after six years and $3.7 billion, the Navy Marine Corps Intranet program had yet to achieve expectations. The report did not place the blame entirely on EDS; it also faulted Navy leadership for failure to implement a plan to monitor how these goals were being met. The failure of NMCI to achieve information superiority and collaboration through interoperability and shared services was cited as a blatant departure from the stated strategic goals of the intranet.

Amid the negative reviews and with a contract in place, the leadership of the Navy began to contemplate the standards and requirements for an information technology network to succeed the multibillion-dollar NMCI after the contract expired in 2010 (Bishnoi, 2006). After contending with the challenges of NMCI, especially the schedule delays and cost overruns, Navy leadership saw the prudence in diligently researching, clarifying and aligning the relationships between IT requirements and the acquisition community so as to best be able to respond efficiently to direction from higher authorities. To this end, the Navy established the Next Generation DON Enterprise Network Core Team with the primary mission of setting goals for follow-on to NMCI. NMCI at this point boasted over 350,000 operational seats and 52 server farms, representing a total of approximately 700,000 users and hundreds of servers dispersed globally. The Navy leadership was beginning to realize that it needed more operational and design control of its networks. Under the terms of NMCI, EDS owned and operated the network and Navy personnel had little or no control; this status quo was one of the challenges that would have to be addressed with the new network. The leadership understood that could not undertake the implementation of an entirely new network. It would have to use NMCI as a “springboard” to the next thing because with NMCI costs at about $1.2 billion a year to run, as well as a legacy networks[6], which cost an additional $1.5 billion, there was not much of a choice (Taylor, 2008).

C. THE NEW BEGINNING

1. Current State of NMCI

The NMCI environment currently boasts over 800,000 NMCI users accounts with more than 400,000 seats transitioned to the end-state NMCI environment in more than 3,000 locations dispersed over seven continents. The network facilitates the transfer of over 3.5 terabytes of data while denying in excess of two million unauthorized access attempts annually. Second only to the Internet in size, and with only four decentralized network-operating centers, the entire intranet is designed to have fail-safe security and redundancy. In spite of all criticism, the network has been instrumental in numerous capacities, such as support of Operation Iraqi Freedom and the war on terrorism, with over 5,000 seats deployed in theater, and it has been instrumental in the formation of hastily formed networks during real world challenges such as Hurricanes Isabel, Katrina, Rita, Dolly, Gustav and Ike. Amidst the late success of NMCI emerge speculations of the need for change and the DON has decided to seek improvements, citing a need for the government to have more control over the network, providing better information assurance and an improved defense posture against looming advancements in cyber-attacks.

In the DON Naval Networking Environment 2016 report released in early 2008, the DON CIO defined the vision, scope, strategy, and concept of operations (CONOPS), for the Department of the Navy’s future Naval Networking Environment in the 2016 timeframe. In the DON NNE-2016 report (2008), Once again it seemed that Navy leadership had underestimated the complexity associated with the transitioning IT and

[6] Limited number of legacy networks were permitted to continue operations as excepted networks running

after exhaustive need analysis, determined that current NMCI management and associated business practices were not optimized to ensure rapid development, testing, and implementation of new information technologies. Both the functional needs analysis and functional solutions analysis showed that the contractor owned/contractor operated network did not allow officials to respond quickly and keep pace with emerging requirements and trends because making changes triggered lengthy and contract negotiations (Castelli, 2010). The solution reached for the current NMCI environment was to change the management and operation of the intranet; the new network termed Next Generation Enterprise Network (NGEN) would be built by incremental buyback of intellectual property from Hewlett-Packard (HP)[7]. The Navy department planned to spend over $1 billion over the next several years in a block-upgrade approach (Castelli, 2010).

The incremental implementation of NGEN was to be phased in without disrupting service to any exiting capabilities, but it had to be in place before the NMCI contract ended in September 2010. Time passed and Navy leadership felt it could not do due diligence in researching, validating and application of industries best practices in acquisition and implementation of NGEN because, after solicitation with the sole-source requirement document, it received only three responses from industry and none of them "indicated an ability to provide the continuation of the NMCI network" (Taylor, 2008). Navy leaders knew that the September 2010 deadline was unattainable and would award a continuity-of-services contract (CoSC) to Electronic Data Systems to keep NMCI online for up to 43 months while the service sought a viable provider for the new network (Taylor, 2010). The contract extension in 2009 with Hewlett-Packard (Now EDS's parent company) valued in excess of $3 billion and gave the Navy time to execute a "controlled" transition to NGEN in a manner that minimized the possible risks to the Navy's IT operations and security. Under the CoSC, HP had to “ensure that the scope of services and performance levels delivered by NMCI in FY10 are sustained until the follow-on NGEN contract is in place and satisfactorily providing the replacement services” (DON,

[7] Hewlett Packard acquired EDS in 2008

2009). CoSC also asserted EDS's continued ownership and operation all of NMCI services in the current environment.

2. Acquisition of NGEN

In the procuring of NGEN, Navy leaders developed an acquisition strategy that allowed for several options and combinations of contracts that could be easily adjusted to meet current and future environments. Navy leaders hoped to increase the current level of command and control with NGEN and to support additional network operations while adjusting to find the compromise between low cost and high performance. To achieve the low costs, the Navy leaders first increased the number of potential providers competing for NGEN by reducing one of the requirements. Previous requirements prohibited companies that did not have previous experience operating more than 100,000 computers on a network. This number was reduced, based on analysis by the NGEN technical and management teams, to a minimum of 40,000 computers on a network (Hudson, 2012a). The low cost goal would also be the impetus for the segmented acquisition of NGEN. The Navy leadership felt that this approach would provide increased competition and promote security as an important part of the contracting process. In an interview, Robert J. Carey, then DON CIO, echoed the belief in the segmented approach:

> We studied the ITIL (Information Technology Infrastructure Library) process and believe it is the most logical way to proceed. Our research indicates that a segmented approach has become an industry best practice over the last few years. Segmenting the work provides greater flexibility for the government and increased opportunities for industry to compete to provide NGEN services (CHIPS, 2008).

The segments to be competed were broken in to five sections: independent security operations oversight and assessment, transport, hardware, software, and enterprise services.

To increase the current level of command and control and visibility of the network, the Navy added over 300 military personnel to facilitate future control of network operations of NGEN. All personnel selected would undergo intensive and function-specific training initially, and periodically as required, to maintain proficiency in their particular position. David Weddel, the assistant deputy chief of naval operations for information dominance in an interview with “Inside the Navy” further explained the Navy’s position

> We’re adding government oversight of over 300 Navy personnel … and the major areas of training will include network operations, security operations and service life-cycle management. As (the government) begins to take control of the Navy-Marine Corps Intranet from contractor HPES, …learning how it's configured, how it's restored, the priority of restoration -- those are things that we will begin to exercise over the network. (Burt, 2010)

The Navy leadership appeared to be on one accord on the expectations of NGEN and on how to acquire them, but the next phase of generating a concrete and final RFP eluded the Navy leaders, adding delays and cost to an already encumbered process.

a. NGEN RFP Delayed

Industry eagerly waited to offer a matching proposal for service in response to the expected RFP from naval leadership about their intended strategy and business objectives for NGEN. On September 30, 2011 Space and Naval Warfare Systems Command released an initial draft request for proposal for the NGEN program. The draft was released instead of a final RFP with the objective that naval leadership could deliver an final RFP in months to come that industry will be able to bid on (Hudson, 2011). After two more delays (five months later than planned), Navy leadership felt that they had to modify the contract and seek additional funding for the NMCI CoSC. Navy leaders were quick to establish that the additional funding was not due to an increase in budget need, requirements, or contract costs, but that additional funds were necessary to maintain NMCI CoSC services through the transition to NGEN. Notwithstanding an RFP delay of about five months, a deadline extension for bids from industry until August 2012, and a price increase of over $2 billion, Navy leaders are still confident that NGEN is still on schedule and will not affect planned program milestones (Hudson, 2012b).

b. Early Transition Activities

In addition to CoSC, Navy leaders hope to guide the transition to NGEN from NMCI with ETAs and new contracts. The ETAs started in October of 2008 to facilitate a successful migration of services from a contractor-owned, contractor-operated model to one that gives the government increased command and control. The ETAs are made up of several initiatives that will establish processes and tools used to lay the groundwork for a seamless transition between NMCI and NGEN (CHIPS, 2010).

D. CONCLUSION

The purpose of this chapter was to walk the reader through the acquisition and implementation of NMCI. The chapter highlights the historical events of the NMCI program, the implementation problems but the main purpose was to give context to subsequent chapter discussions.

The next chapter deals with the ETA and follow-on contracts used by DON officials to acquire and transition to NGEN. It will provide in-depth description of what they are and their intended purpose as well as the effectiveness of the ETA and the overall transition from the NMCI to the NGEN environment.

III. EARLY TRANSITION ACTIVITIES AND CONTRACTS

A. EARLY TRANSITION ACTIVITIES

This chapter highlights the ETA and follow-on contracts to give an in-depth description of what they are and their intended purpose. This chapter also evaluates the effectiveness of the ETA and the overall transition from the NMCI to the NGEN environment.

The previous chapter charted the transition process from the disparate networks to an integrated NMCI environment. The transition was severely impeded by the unexpectedly high number of legacy systems and by resistance from the stakeholders. The resistance from the stakeholders, that is, the negative end user response and repeated attacks from the legislative branch of the government, was the greatest impediment for the transition. With regard to the problematic NMCI implementation and considering the current rate of failure for transitions in organizations in recent history is between 50% and 70% (Pasmore, 2011), the transition has been largely successful but nowhere near perfect. Navy leaders understand that with a near $3 billion a year in operating cost ($1.2 billion a year to run NMCI and $1.5 billion to run existing legacy networks), it must increase its control of the new Network (Taylor, 2008). In 2009, with intentions to transition from NMCI to NGEN, Navy leaders leveraging lessons learned from the NCMI transition began to develop ETAs to prepare for a successful migration of services from a contractor-owned, contractor-operated model to one that gives the government increased command and control (GAO, 2011). The eight ETAs are intended to be the foundational efforts to

- establish government management capabilities;
- allow greater participation in decisions;
- support full and open competition for services; and
- reduce risk through expedited transition times.

Successful transitions are product of a deliberate approach to the process that includes, but is not limited to, effective communication between all stakeholders and clearly stated goals and objectives. With the ETAs, DON officials plan to mitigate the risk of migration to the NGEN segmentation service model for both industry and the government.

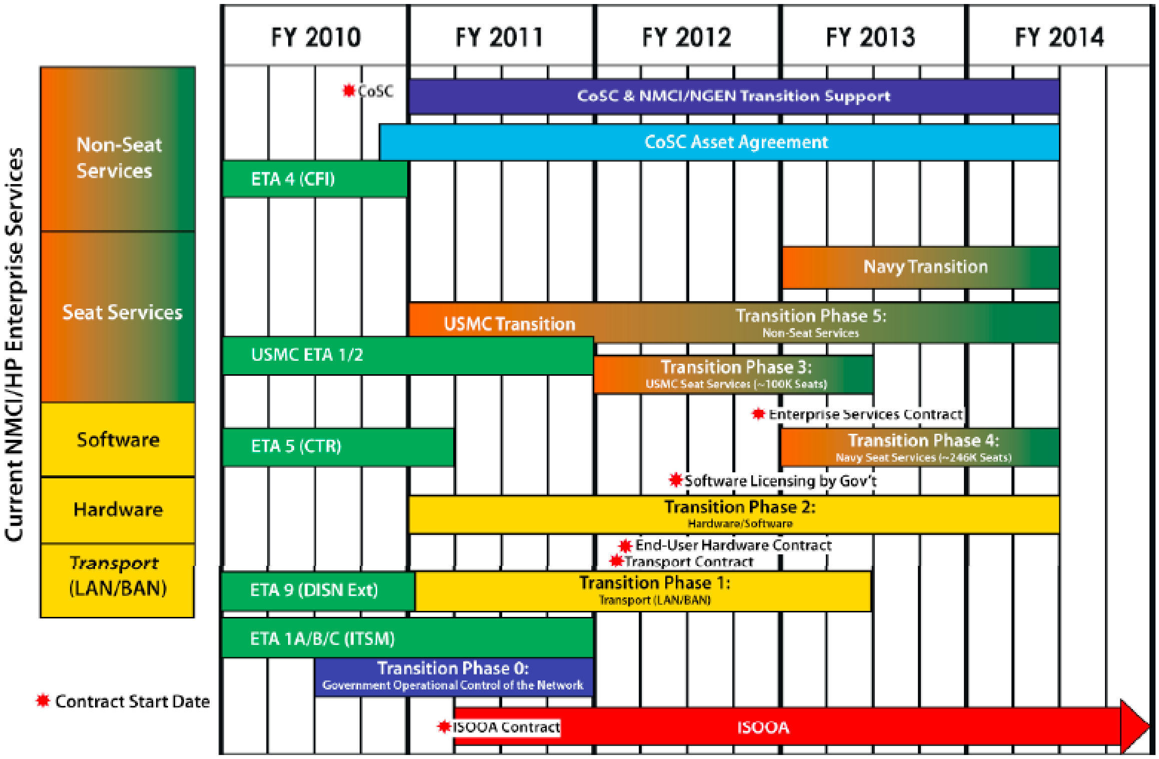


Figure 1. Macro View of Transition Activities and Contracts for NGEN (From Holland, 2010)

NGEN is expected to be developed incrementally, and as of September 30, 2010, the NGEN program had reportedly spent about $432 million, with the first increment to provide comparable NMCI capabilities, additional information assurance, and increased government control of the network (GAO, 2011). The current budgeted amount for the first increment is about $50 billion, and future cost estimates for subsequent increments have yet to be defined. Figure 1 provides a macro view of the ETAs and the contracts. The subsequent paragraphs provide an in-depth description of the ETAs and contracts, however it is important to know the ETAs are not listed in any particular order as some of the activities and contracts were executed concurrently.

Table 1. Early Transition Activities (After GAO, 2010)

Early transition activity	Start date	End date	Cost (in millions)	Description
Information Technology Service Management Process Development	Oct-08	May-11	$20.50	Develop Information Technology Infrastructure Library a version 3-based service strategies, processes, and procedures.
Contractor Technical Representative Workforce Reconstitution	Jan-09	Apr-11	$3.30	Conduct job task analysis and assess learning tools for contractor technical representatives; develop enterprise-wide position descriptions and occupational standards for training, advancement, criteria, and performance objectives.
Comprehensive Facilities and Infrastructure Inventory	Jan-09	Dec-10	$12.00	Evaluate, analyze, and validate current NMCI infrastructure inventory consisting of technical data, assets, configuration items, and system components.
Defense Information System Network Core Extension Phase 1 and Maritime Operation Center Implementation	Apr-08	May-11	$6.70	Bring consistent wide area network connectivity from the Defense Information System Network to eight major nodes at fleet headquarters (Norfolk, Virginia, and Pearl Harbor, Hawaii).
Global Network Operations Command and Control Workforce Establishment	Oct-08	Jul-11	$14.30	Develop the personnel, processes, and tool requirements, and organizational analysis and alignment.
Wide Area Network and Enterprise Services Upgrade	Apr-09	Aug-12	$46.00	Demonstrate network operational control capability and validate the NGEN System Design baseline through early implementation.
Enterprise Tools Strategy and Implementation/Integration	Apr-09	May-11	$56.60	Analyze current tool capabilities to support information technology service management processes, and develop design requirements and tool integration specifications.
Non-classified Internet Protocol Router Network Migration – Marine Air-Ground Task Force IT Support Centers East Pilot	Oct-09	Aug-11	$12.90	Assess the transition of base area network, local area network, and end-user equipment for about 1,200 users from the continuity of services contract to the government-owned/government operated NGEN environment.

1. ETA 1A: Information Technology Service Management (ITSM) Process Development

Navy leadership has adopted several measures to ensure operational control across its IT enterprise as it prepares for a full and open competition of NGEN services. One of the ETAs used to lay the groundwork for a smooth transition is the decision to enhance its insights of proven industry standards such as information technology service management (ITSM). ITSM is a set of actions that are concerned with the delivery and support of IT services that are appropriate to the business requirements of an organization (Addy, 2010). ITSM seeks to standardize the business process, activities and roles; common definitions are established in documents, repeatable procedures are implemented, and clearly defined roles for all stakeholders are established. To improve deficiency resolution, ITSM process focuses on the quality of service offered to the user by evaluation of quantifiable and technical metrics determined from IT characteristics such as throughput and response time.

The ITSM process will be based on current industry information technology infrastructure library (ITIL V3) standards. ITIL V3 is the latest iteration of what has become an international standard or library of a cohesive set of best practices for information technology service management drawn from the public and private sectors worldwide (Cervone, 2008). The standards and procedures listed in the ITIL V3 are entirely generic and DON intends to apply the process and procedures to support its controlled network operations and management. The NGEN Requirements Task Force in the *Next Generation Enterprise Network (NGEN) Requirements Document (2008)*, acknowledged the absence of standards for ITSM implementation. The task force further accentuated the dependence of successful implementation of IT service management on established IT governance and IT support.

IT governance will be pivotal in the centralized oversight of knowledge management, service asset, and configuration management, event management and portfolio management. Currently the IT governance is a joint effort between the NGEN program office and the Naval Network Warfare Command to ensure adequate government oversight, IT conformance, and standardization and integration of processes across all segment of the NGEN environment. Standardization and integration of the processes synchronizes ITSM's effort at enterprise level, which creates an avenue for compliant and repeatable procedures that can be incorporated in training specifications for the government and contractors (CHIPS, 2010). This process mitigates duplication and stove-piped efforts and leads to consistency of ITSM operations across NGEN stakeholders.

Although DON leaders have assigned program life cycles with specific funds and managed by an integrated product team (IPT), the information technology service management process development effort estimated at over $20 million dollars and a duration of three years after the start date in October 2008 will continue until NGEN reaches its full operating capability (CHIPS, 2010).

2. ETA 4: Comprehensive Facilities & Infrastructure Inventory

This ETA entails a comprehensive facilities and infrastructure inventory that seeks to evaluate, analyze, and validate current NMCI infrastructure inventory consisting of technical data, assets, configuration items, and system components. Navy leaders believe this to be one of the vital ETAs because it will adequately inform the NGEN request for information/request for proposal activities by creating a comprehensive asset database of NMCI's core infrastructure (CHIPS, 2010). The process will capture the information necessary to establish an enterprise infrastructure asset baseline of the current NMCI infrastructure. This process, commonly referred to as IT asset management (ITAM), is part of the guidance from the ITIL V3 procedures and it involves the complete inventory of all IT assets, to include but not limited to:

- All IP enabled, networked devices
- Device operating systems and types (servers, desktops, printers, routers, IP-enabled devices)
- System configuration data (CPU, memory, serial number, etc.)
- Installed software and services (vendor, version, patch level)
- Software application and database users and usage rate (application, users, etc.)
- Server utilization rate (NGEN, 2008a)

ITAM is fundamentally the collection of on-hand hardware and software inventory information intended to facilitate future hardware and software purchases and redistribution. The application of ITAM not only ensures that all assets are accounted for, but also assesses the capabilities and the limitations as well as verifies efficient use of all assets. DON will utilize asset management to determine the level and value of its ready-to-use assets. According to the *Next Generation Enterprise Network (NGEN) Requirements Document (2008)*:

> ITAM will be employed to inventory Navy enterprise IT networks on a recurring basis to maintain accuracy, capture mobile or temporarily off-line assets, and identify trends in configuration changes. Detailed and comprehensive data for networked assets will be automatically collected and reported via secure communications protocols and ports and then stored in a centralized repository under control of the government in accordance with appropriate government security classification guidelines. (DON, 2008a)

DON believes the ITAM process is vital to NGEN and the move to a consolidated management environment. Its application will aid in mitigating the excessive costs and providing better visibility for monitoring and management of the enterprise (CHIPS, 2010). To that end, the assessment, implementation and integration process was budgeted at over $56 million; the highest amount budgeted for the ETAs.

3. ETA1B: Tools Strategy and Implementation/Integration

This is a follow-on to the comprehensive facilities and infrastructure inventory and utilizes inventory information to determine how best an asset can be configured into the larger networked enterprise. The goal of this ETA is to analyze current tool capabilities to support ITSM processes, and develop design requirements and tool integration specifications that lead to technical solutions. This process is also rooted in the ITIL V3 procedures under the service asset and configuration management (SACM).

Under the ITIL V3, SACM consists of an iterative process of configuration identification, configuration control, configuration verification and audit. The ITIL V3 procedure for SACM defines the initial structure of the configuration model by defining all configuration items (CIs) and their sub-components, as well as determining their interrelationships (ITIL, n.d.). This base configuration is then documented in the configuration management system to ensure that any future changes are consonant with the base system. The iterative portion of SACM is the configuration verification and audit, and it is executed by performing regular checks to ensure that the information contained in the configuration management system is an exact representation of the CIs actually installed in the live production environment.

Navy leaders acknowledge its ambitious task of SACM as they seek to synchronize NGEN, first into the Naval Networks Environment Family of Systems, and further down the line with the Global Information Grid; the System of Systems. NGEN Requirements Document (2008) argues that the application of SACM is within this system of systems, and family of systems construct is critically important to enable the operation of legacy and emerging applications, systems, and services within a DoD and DON net-centric enterprise and to support warfighter mission requirements from end-to-end. Adequate attention to validating requirements and the configuration of NGEN as it pertains to capabilities and interoperability will pay a great dividend with respect to systems integration.

4. ETA 1C: Global NetOps C2 Workforce Establishment

Started in January 2009, this ETA seeks to bridge the gap between current manning and the desired level for the effective operation of NGEN. DON leadership understands that current personnel are not sufficiently trained to meet the needs required to have adequate oversight in a government-owned networked environment, given its size and complexity. *Next Generation Enterprise Network (NGEN) Requirements Document (2008a)* identifies the gap as a combination of the number of personnel and degree of competency in technical and process maturity capability (p.5).

The activity will develop enterprise-wide position descriptions and occupational standards for standardized training, advancement criteria and performance objectives based on DoD Directive (DoDD) 8570.01-M, the premier document for guidance on DoD Information Assurance Training, Certification, and Workforce Management. DoD 8570.1-M (2007) identifies and categorizes positions and certification of personnel conducting information assurance (IA) functions within the DoD workforce supporting the DoD global information grid (GIG) in accordance with overarching DoD directives.[8] The requirement for adequate workforce began as a phased approach in 2005, and after its fourth year it mandates that all IT initiatives must be in 100% compliance with 8570.1M, further specifying that the DoD requires approximately 110,000 identified IA professionals to be certified.

In order to assure that the NGEN Workforce is DoD 8570 1 compliant, DON leadership plans to conduct a job task analysis and assess learning tools for contractor technical representatives to develop enterprise-wide position descriptions and occupational standards for training, advancement, criteria, and performance objectives (GAO, 2011).

5. ETA 9: Defense Information System Network Core Extension Phase 1

DON leadership understands to operate and sustain NGEN, a highly complex and large system, it must first develop and fortify a resilient, robust and consistent wide area network. The leadership feels that the first step in this process is to identify external and internal factors that affect the network, and then these factors have to be evaluated and assessed for levels of risk. *Next Generation Enterprise Network (NGEN) Requirements Document (2008)* identified the two major external factors affecting the proposed NGEN networks as electric power supply and availability of DoD-provided services on the Defense Information System Network (DISN) (p. 50). The availability of services such as graceful degradation, dynamic rerouting, and end-to-end protection, and the denial of electrical power will have a significant, if not critical, impact on NGEN availability.

To improve the infrastructure already in place, DON will increase connectivity from the DISN to eight major nodes at fleet headquarters (Norfolk, Virginia, and Pearl Harbor, Hawaii) by deploying DISN WAN with intent of enhancing quality of service for tactical and non-tactical areas of NMCI/NGEN (Holland, 2010). *NGEN Requirements Document (2008)* recommends a development of assessment plans to identify all data collection on specific nodes and linkages using appropriate measurements of effectiveness (MOE) and measurements of performance to capture how effective NGEN

[8] DoD Directive 8000.1, “Management of DoD Information Resources and Information Technology,” February 27, 2002 and DoD Directive 8500.1, “Information Assurance,” October 24, 2002

is in its support of the naval user community. This ETA was scheduled to begin in April of 2008 with duration of three years and at a budgeted cost of $6.7 million dollars.

6. ETA 5: Contract Technical Representative (CTR) Workforce Reconstitution

The goal of this ETA is to map the transition of a contractor-operated environment to a government-controlled environment by doing an "AS-IS" work analysis and manpower development process currently in play to align the contract technical representative workforce with NGEN acquisition and mission strategies. The analysis will identify current roles and define future define NGEN CTR roles and responsibilities, as well as training requirements, to meet NGEN performance expectations.

Navy leaders will use contractors already in place during the transition to ensure required support during initial operational capability (IOC) equipment installation and operations. The transition to government owned and operated will be phased in and based on the mandated performance-based business environment; performance-based logistic documents which mandate will be provided by current trained and certified contractors to satisfy sustainment support requirements for IOC to the degree practical. The *NGEN Requirements Document (2008)* mandates contractor logistics support as the standard approach for IOC due to the few number of government (Navy and civilian) personnel trained and validated to use and maintain NGEN.

7. USMC ETA 1: USMC Upgrade WAN & Implement Enterprise Services

According to the *NGEN Network Operations (NetOps) and Concept of Operations (CONOPS)* (2008), the 85,000 unclassified seats currently supported by NMCI services on USMC installations will be transitioned to the NGEN environment. The USMC ETA (1) will replace and refresh exiting Marine Corps enterprise network (MCEN) infrastructure items at each Marine Air-Ground Task Force (MAGTF) IT Support Center (MITSC). MITSCs are generally provisioned within a Marine Corps Installation Commands to support Marine Expeditionary Force Commands and, as part of the fifth element of the MAGTF, to support the warfighter while operationally deployed, in garrison, or engaged in training. After the MITSCs have been updated, they will be validated to the standards of the NGEN system design baseline and demonstrate network operational control capability through early implementation. The upgrade of MCEN to NGEN at all the MITSCs is budgeted for $46.00 million.

8. USMC ETA 2: USMC NIPRNET Migration - MITSC East Pilot

Under the NGEN environment, the network will be divided into two management domains (MDs). The MDs set the boundaries within NGEN for management authority for purposes of command and control. This ETA provides guidelines for Marine Corps Network Operations and Security Command, the USMC NGEN MD, as the marines transition enterprise seat services from the incumbent vendor to a government-owned/ government-operated model. This pilot program involves the assumption of control on the base area network (BAN), the local area network and the migration of end-users to the Marine Corps Worldwide Active Directory, management and sustainment processes, and the transition of user workstations for approximately 1,200 users. (CHIPS, 2010)

Naval leadership intends to spend $12.90 million to implement the pilot program after the upgrade and validation of the MITSC at Camp Lejeune, Marine Corps Installations Headquarters East. This pilot program will undergo a full operational capability test and evaluation, and any lessons gleaned will serve as a model for the entire Marine Corps.

B. CONTRACTS

GAO report (2012a) asserts the Office of the Secretary of Defense gave acquisition approval of the NGEN with an emphasis on segmentation of the network elements. Each segment represents an allocation of IT services, functions, tools, and roles and responsibilities associated with end-to-end service delivery that will be provided by contractors or government sources fielded through multiple competitive awards. The Navy leadership understands segmentation of the network creates seams that must be managed effectively to ensure successful delivery and continuity of services. The two primary segments expected to be awarded are enterprise services and transport services and the remaining three segments are end user hardware; enterprise software licenses, and independent security operations, oversight and assessment support.

1. Contract for Transport Services

This contract was awarded to provide for the operation and sustainment of the transport infrastructure, associated services, and level-of-effort support for those services. Transport infrastructure includes items such as cables, routers, and switches, and end-user equipment such as computers, monitors, keyboards and software. Further definition of Transport Services extends to devices and hardware that provide data storage, transport of voice and data, and video teleconferencing. Included in the contract is the provision to provide technology refresh of cable plant, routers, and switches; some leasehold improvements; and moveable infrastructure associated with local network operations. The contract will be in consonance with aforementioned asset management and will provide infrastructure as government furnished equipment.

2. Contract for Enterprise Services

With the enterprise services contract, DON leaders will seek to understand and integrate the complex and diverse applications and data of the current NMCI environment, and finally to integrate end-user seat components, especially the hardware. As the premier integration tool in NGEN, the contract is designed to cover coordination across all vendors for the successful delivery of NGEN services. The contract will also provide the enterprise service desk, seat services supporting end user devices, and data center services such as storage and e-mail, along with hardware and software specific to current enterprise services that are not covered under the end user hardware and enterprise software licenses segments (GAO, 2012a).

Though still viewed as separate segments, DON officials will procure the transport and enterprise services segments simultaneously in order to potentially reduce labor costs, administrative burdens, and risk. DON officials identified both transport and enterprise services as fundamentally related under NMCI, and will award a combined contract for both segments (GAO, 2012a). The report further states the transport and enterprise services segments will be awarded simultaneously after approval of Milestone C decision DON instead of staggering their implementation.

3. Contract for Enterprise Software Licenses

This contract will provide software licenses for government purpose rights license for NMCI technical data, computer software, and computer software documentation as part of the ETA and to meet DON-wide requirements. Use of enterprise license agreements (ELAs), where available, is mandatory by all DON organizations and programs with the release of a joint DON memo (DON ELA 2012). These enterprise agreements optimize cost savings by leveraging the full purchasing capacity of the department. The contract will require that all software for NGEN be procured as commodities through the DoD Enterprise Software Initiative[9]. The contract will ensure the maximum use of DoD-standards-compliant software and commercial-off-the shelf products for NGEN.

4. Contract for End-User Hardware

For this contract, DON officials will use two different approaches for the USN and USMC domain. According to GAO report (2012), DON officials will acquire end user hardware as a service from the enterprise services contractor rather than purchase the equipment and provide it as government-furnished property to the contractor. The initial plans was to acquire existing end user hardware owned by the incumbent and provide it to the enterprise services contractor as government-furnished property or acquire the end user hardware from the enterprise services contractor as a service. The Marine Corps will obtain end user hardware from Marine Corps common hardware suite as part of the government-owned and government-operated mode of the delivering NGEN services. The requirement for both the USN domain and USMC domain, however, is that all components acquired have to comply with DoD policies and regulations, and satisfy commercial and international standards set forth by the Institute of Electrical and Electronics Engineers.

[9] The Enterprise Software Initiative (ESI) is a joint DoD project to develop and implement a DoD enterprise-wide Software Asset Management process.

5. Contract for Independent Security Operations Oversight and Assessment (ISOOA)

The ISOOA contract was originally envisioned as services to be provided by an independent third-party security provider for the NMCI environment as it transitioned to NGEN within the USN domain, and for organic Marine Corps forces to provide USMC security functions (GAO, 2012a). With recent changes in the acquisition approach, the USN is no longer expected to award a contract for the verification, validation, and reporting segment because the Navy now has an internal entity—the 10th Fleet/Cyber Command[10] (GAO, 2012a). The USMC will continue to perform its security operations oversight and assessment.

With the ETAs and the contracts, the naval leaders proceeded to move from the current NMCI construct to NGEN, promising that the best possible levels of service quality and availability would be sustained. NGEN is envisioned as a network-centric force multiplier for the warfighter by facilitating a secure, reliable, and adaptable global information exchange across the full spectrum of operations. The ETAs have a spiral development process ensuring that problems are identified and addressed rapidly, and the segmented approach award system is an attempt to acquire NGEN at the "best value" using the lowest price technically acceptable (LPTA)[11] as basis for award.

[10] The U.S. Fleet Cyber Command / U.S. 10th Fleet is a functional formation of the United States Navy responsible for the Navy's cyber warfare programs.

[11] Based on FAR 15.101–2… which states (a) the lowest price technically acceptable source selection process is appropriate when best value is expected to result from selection of the technically acceptable proposal with the lowest evaluated price.

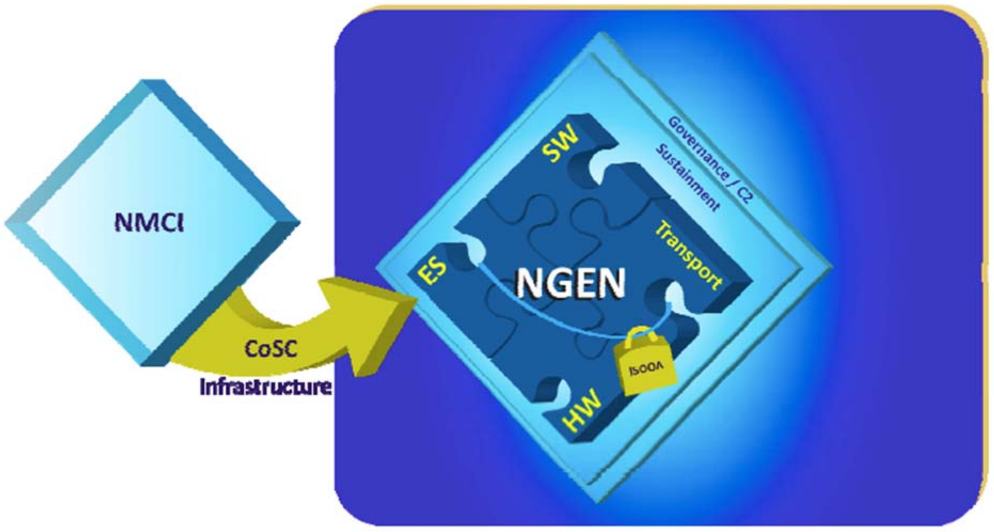


Figure 2. NGEN Segmented Solution (From Holland, 2010)

According to DON program officials, the decisions to proceed with the transition were based on their view that all the efforts had sufficiently mitigated known risks and issues considering the length of the transition process, albeit one laden with complexities, and taking into account the sheer magnitude of the network (GAO, 2010).

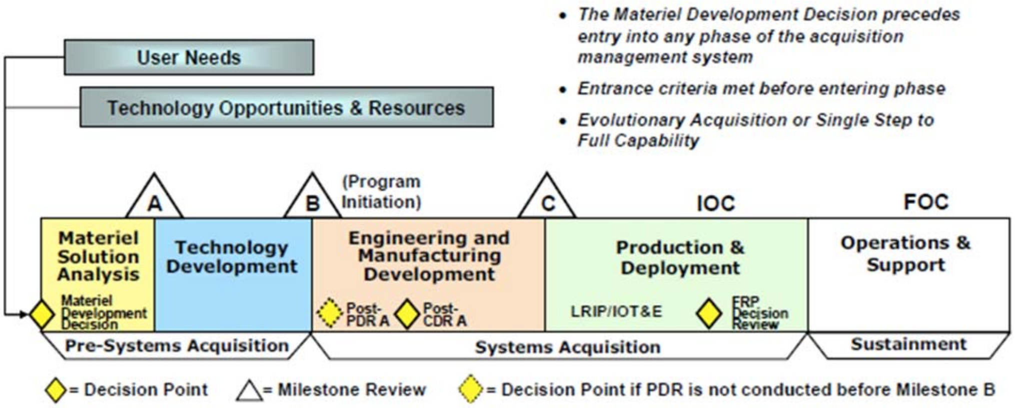
As of the time of the GAO report dated September 2012, the transition is plagued with schedule delays and it seems unlikely that the DON will fully transition to NGEN by the end of the continuity of services contract in April 2014.

C. GAO ASSESSMENT

As the audit, evaluation, and investigative arm of the United States Congress, the GAO was directed by Congress to ensure the DON had sufficiently analyzed alternative acquisition approaches and had demonstrated that a reliable schedule for executing the program was in place. Furthermore, DON was to show that its program acquisition decisions were grounded in DoD performance and risk-mitigated methods (GAO, 2010). To do this, GAO personnel reviewed the NGEN analysis of alternatives (AoA),[12]

[12] Analysis of alternatives is the analytical comparison of multiple alternatives to be completed before committing resources to one project.

integrated master schedule, and key milestone[13] decisions. Figure 4 gives an overview of the acquisition life cycle process with the different milestones.



User Needs
Technology Opportunities & Resources
• The Materiel Development Decision precedes entry into any phase of the acquisition management system
• Entrance criteria met before entering phase
• Evolutionary Acquisition or Single Step to Full Capability
A
B
(Program Initiation)
C
IOC
FOC
Materiel Solution Analysis
Technology Development
Engineering and Manufacturing Development
Production & Deployment
Operations & Support
Materiel Development Decision
Post-PDR A
Post-CDR A
LRIP/IOT&E
FRP Decision Review
Pre-Systems Acquisition
Systems Acquisition
Sustainment
= Decision Point
= Milestone Review
= Decision Point if PDR is not conducted before Milestone B

Figure 3. Acquisition Process with Milestones Overview (From DAU, n.d.)

In the subsequent report, GAO officials showed that though DON officials had well-documented cost estimates, the overall NGEN acquisition approach was not grounded in a reliable analysis of alternatives approach, the timely execution of the program was lacking due to a poorly derived integrated master schedule and this culminated in patterns of missed milestones, and delays in key program documentation and gate review decisions.

1. Analysis of Alternatives (AoA)

According to *Defense Acquisition University: Introduction to defense acquisition management* (2008) analysis of alternatives (AoA)

> …is a process that assesses and evaluates potential materiel solutions with intentions to satisfy the requirements or needs documented in an approved Initial Capabilities Document (ICD). It focuses on identification and analysis of alternatives, measures of effectiveness (MOE), cost, schedule, concepts of operations, and overall risk, including the sensitivity of each alternative to possible changes in key assumptions or variables. The AoA also assesses critical technology elements (CTE) associated with each

[13] Milestones are a point in time where a recommendation is made to the Milestone Decision Authority (MDA) about starting or continuing an acquisition program into the next phase. DoDI 5000.02 "Operation of the Defense Acquisition System" establishes the milestones and milestone requirements.

> proposed materiel solution, including technology maturity, integration risk, manufacturing feasibility, and, where necessary, technology maturation and demonstration needs. (DAU, 2008)

During Gate 2 of the DON review process done concurrently with the DoD materiel solution analysis (MSA), the findings from pertinent AoA are used to approve the preferred alternatives resulting from the analysis. For the acquisition of NGEN the Director, Cost Assessment and Program Evaluation, Office of the Secretary of Defense (OSD CAPE), issued the NGEN AoA guidance, reviewed the AoA study plan, and approved the AoA results.

GAO determined that DON and DoD officials failed in executing an effective AoA because (1) it contained key weaknesses in its cost estimation, and (2) it did not sufficiently assess operational effectiveness. These two fundamental disadvantages impaired DON officials' ability to inform investment decision-making.

a. Cost Estimation Weakness

As a core tenet of AoA, the evaluation of the potential cost expected is vetted on the premise that the alternative chosen is sound and proven, and also that it has the met the requirement of being the "lowest price technically acceptable." The GAO report (2011a) argued that the method of cost estimation for the chosen alternative was flawed because it did not use historical records that cited actual cost and schedule experiences on comparable programs. This failure to make grounded estimates and the consequent approval by OSD CAPE, which had concluded that the DON's AoA was sufficient, led to designation of the first increment of NGEN as a major automated information system (MAIS)[14] (GAO, 2010). The cost estimation analysis was to determine the extent to

[14] Designation for all systems of computer hardware, computer software, data and/or telecommunications that perform functions such as collecting, processing, storing, transmitting and displaying information that exceeds $378 million (FY 2000 constant dollars) for all expenditures, for all increments, regardless of appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the MSA phase through sustainment for the estimated useful life of the system.

which AoA had measured up to the four characteristics[15] of a reliable estimate promulgated in GAO's *Cost Estimating and Assessment Guide*.

The GAO report (2010) concluded that DON officials had a well-documented AoA with a defined purpose of the estimate to include program background, system description, disclosed ground rules and assumptions, but failed to deliver a comprehensive analysis that included all government (e.g., personnel) and contractor costs over the program's full life cycle (from inception to retirement). Instead, the DON officials provided analysis on government and contractor costs for a five-year period from fiscal year 2011 to fiscal year 2015. DON officials also failed to provide accurate estimates; though based on NMCI historical cost data and adjusted for inflation, the estimates contained mathematical mistakes and were largely grounded in documented assumptions. Attempts to verify accuracy were thwarted due to the proprietary data of the contractor being used for the independent government review. The final cost estimation weakness was attributed to the lack of credibility due to quality of data used. The data used to conduct analysis was often based on the contractor's experience and not an independent third party observation. In response to the claim by GAO analysis, lower level officials blamed the discrepancies on insufficient time given to conduct a more thorough analysis.

b. Insufficient Assessment of Operational Effectiveness

According to DoD regulations[16] governing proper analysis of alternatives, all assessments must include identification of core operational capabilities and goals to be achieved by the system solution, establishment of quantitative or qualitative measures (or both) for evaluating the operational effectiveness of each alternative, and a definition of each alternative metric to evaluate the ability of the alternative to meet the measures established.

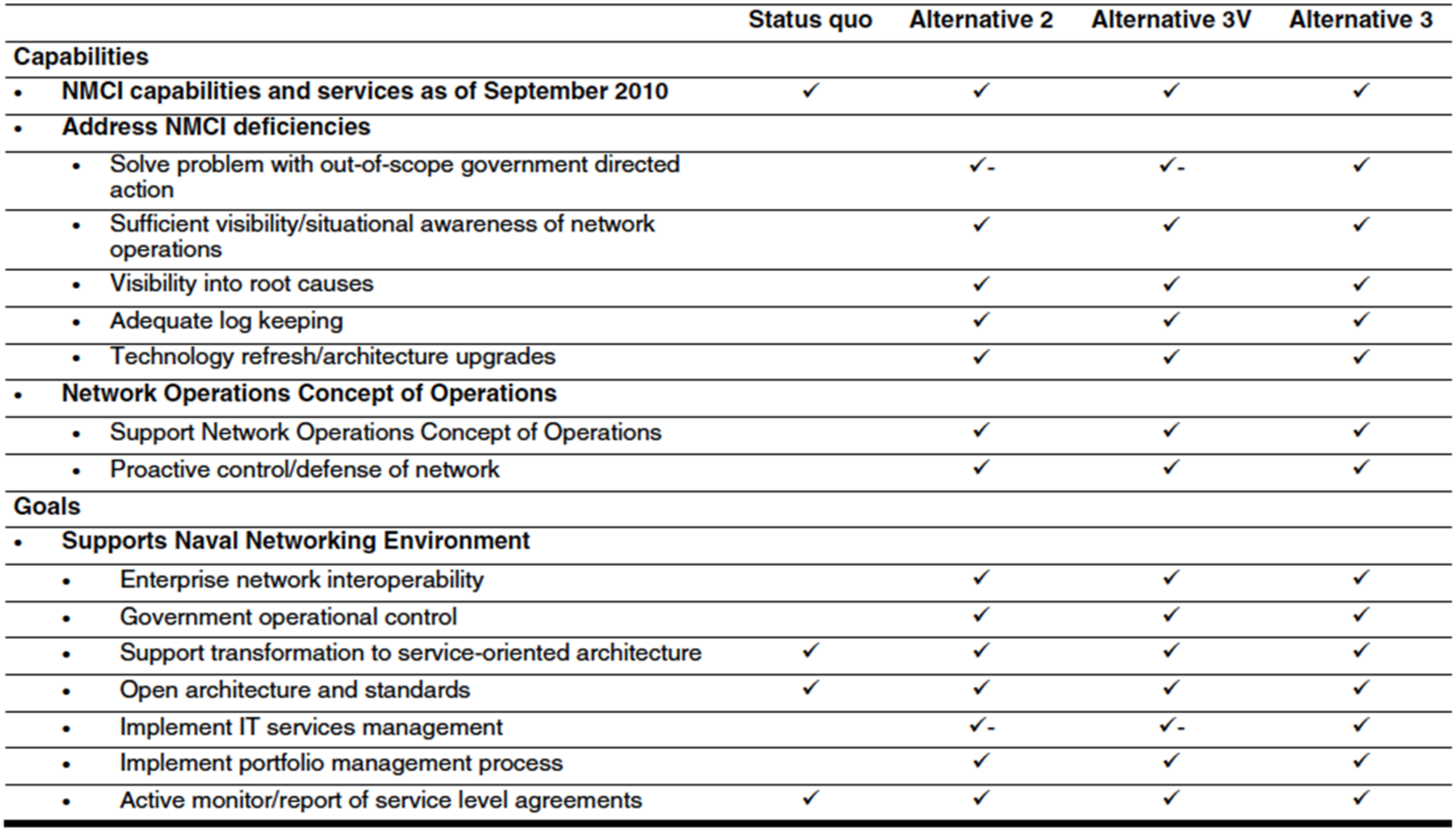
[15] Determines if a cost estimate is well documented, comprehensive, accurate, and credible.

[16] *Defense Acquisition Guidebook*; Section 3.3 "Analysis of Alternatives" (Mar. 19, 2010); *DON Acquisition and Capabilities Guidebook* (December 2008).

GAO report (2010) credited DON officials for identifying the capabilities and goals that the NGEN system solution should achieve, but claimed the analysis fell short in establishing quantitative and qualitative measures for the capabilities identified. Instead it compared the alternatives based on qualitative determinations of whether the capability or goal was either met or partially met. DON officials accountable for developing the AoA attributed the inadequate operational effectiveness analysis to time constraints brought on by the demands for a timely delivery of the requests for proposals.

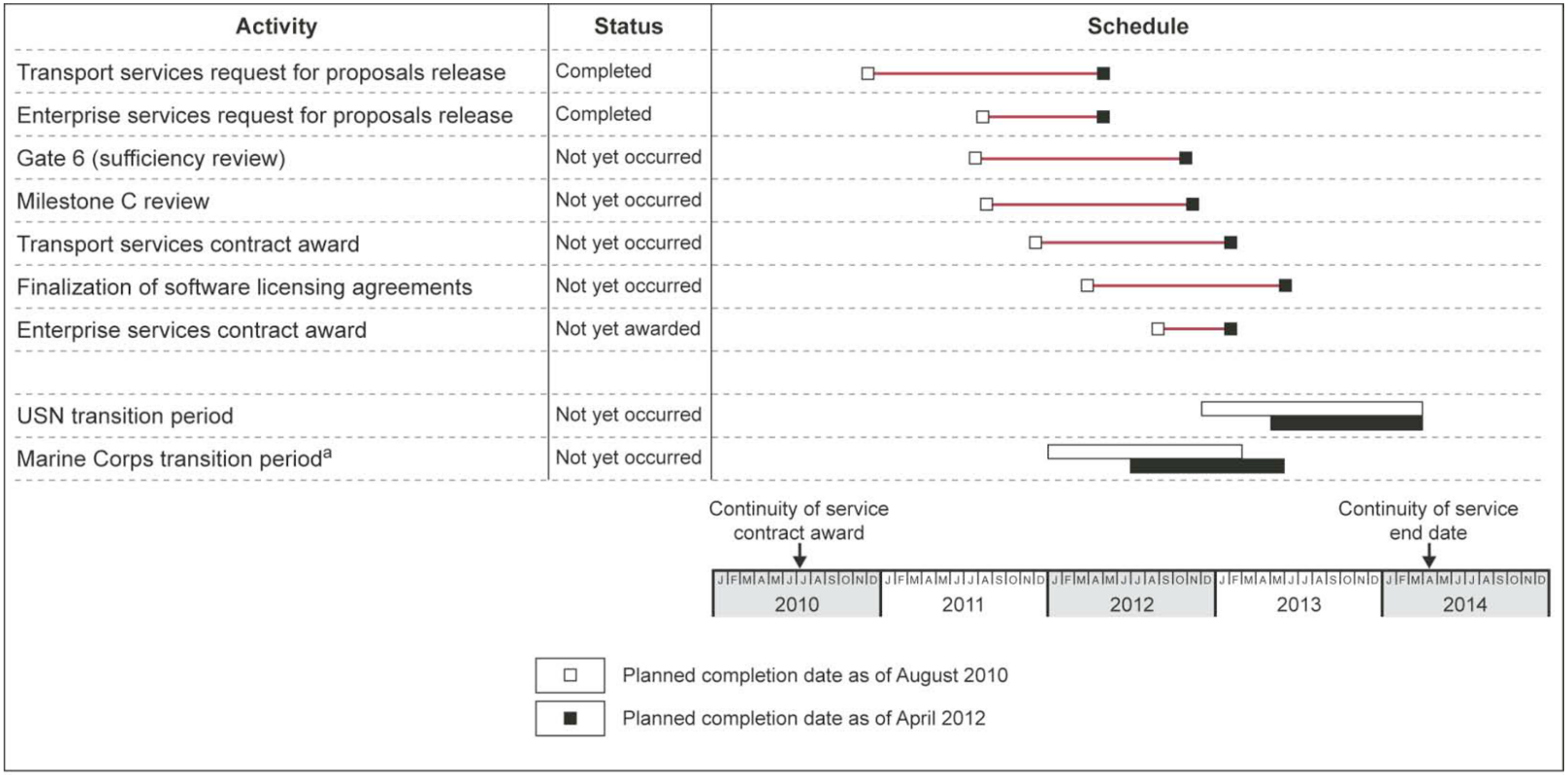
GAO officials maintained their position on the failure of DON and DoD officials executing an effective AoA because of the weaknesses in cost estimation and insufficient assessments of the operational effectiveness and further cited the shortcomings of a time-constrained approach to analysis of alternatives. GAO officials also argued that the scope of an alternatives analysis should be proportionate to the amount of resources affected by the decision, with more significant programs receiving more analytical attention, an approach grounded in DoD guidance (GAO, 2011a)

Top DON and DoD officials immediately refuted time constraint statements by GAO with OSD officials stating that the differences between the current approach and the alternatives that were assessed are, in their view, insignificant. Without a credible AoA and with a nebulous assertion to increased flexibility among the alternatives, DON officials went on to select a segmented approach to provide the touted increased flexibility in meeting NGEN capabilities and goals with no additional cost. GOA officials still maintain the current approach is estimated to cost at least $4.7 billion more than any of the AoA alternatives (GAO, 2010).



	Status quo	Alternative 2	Alternative 3V	Alternative 3
Capabilities				
• **NMCI capabilities and services as of September 2010**	✓	✓	✓	✓
• **Address NMCI deficiencies**				
• Solve problem with out-of-scope government directed action		✓-	✓-	✓
• Sufficient visibility/situational awareness of network operations		✓	✓	✓
• Visibility into root causes		✓	✓	✓
• Adequate log keeping		✓	✓	✓
• Technology refresh/architecture upgrades		✓	✓	✓
• **Network Operations Concept of Operations**				
• Support Network Operations Concept of Operations		✓	✓	✓
• Proactive control/defense of network		✓	✓	✓
Goals				
• **Supports Naval Networking Environment**				
• Enterprise network interoperability		✓	✓	✓
• Government operational control		✓	✓	✓
• Support transformation to service-oriented architecture	✓	✓	✓	✓
• Open architecture and standards	✓	✓	✓	✓
• Implement IT services management		✓-	✓-	✓
• Implement portfolio management process		✓	✓	✓
• Active monitor/report of service level agreements	✓	✓	✓	✓

Figure 4. DON’s Qualitative Assessment of Alternatives’ Ability to Meet NGEN Capabilities and Goals (From GAO, 2010)



Activity	Status
Transport services request for proposals release	Completed
Enterprise services request for proposals release	Completed
Gate 6 (sufficiency review)	Not yet occurred
Milestone C review	Not yet occurred
Transport services contract award	Not yet occurred
Finalization of software licensing agreements	Not yet occurred
Enterprise services contract award	Not yet awarded
USN transition period	Not yet occurred
Marine Corps transition period[a]	Not yet occurred

Schedule
Continuity of service contract award
Continuity of service end date
J F M A M J J A S O N D
2010
2011
2012
2013
2014
□ Planned completion date as of August 2010
■ Planned completion date as of April 2012

Source: GAO analysis of DON data.

Figure 5. NGEN Major Milestone Delay (From GAO, 2012)

c. *Untimely Execution*

As of December 2011, DON officials reported a completion of all ETAs; the several initiatives that sought to define processes and tools used to lay the groundwork for a seamless transition between NMCI and NGEN. At the time of the GAO 2012 report on NGEN, several of the contracts that were intended to facilitate the actual delivery of services for NGEN had been delayed several months, severely undermining ability to fully transition by the end of the continuity of services contract in April 2014.

Program officials blamed the delays to the NGEN program on the need for additional planning, constraints with staffing limitations, and frequent revisions to the request for proposals, and they feared that the program transition from its existing system to NGEN would face further delays and cost overruns. GAO officials concurred with the high probability of future delays, citing previous reviews that revealed an absence of a reliable schedule for executing NGEN. In previews review, GAO claimed the DON schedule for the program execution failed in comparison to best practices associated with developing and maintaining a reliable schedule. The review suggested the effective implementation of the best practices revealed critical paths that increased the probability of negating delays associated with the completion of NGEN events and milestones, including multiple major acquisition reviews and program plans. Review of the schedule for NGEN execution revealed only two of the four sub schedules adequately satisfied any of the nine practices[17] that are associated with developing and maintaining a reliable schedule (GAO, 2010).

[17] The nine best practices identified aid in developing and maintaining reliable schedules for interdependent and complex projects. These are (1) capturing all activities, (2) sequencing all activities, (3) assigning resources to all activities, (4) establishing the duration of all activities, (5) integrating schedule activities horizontally and vertically, (6) establishing the critical path for all activities, (7) identifying reasonable "float" between activities, (8) conducting a schedule risk analysis, and (9) updating the schedule using logic and durations.

d. Segmented Approach

DON officials chose to use a segmented approach to acquiring IT services through the competitive award of multiple contracts for local transport, hardware, software and enterprise services. The decision was based on best practices currently used by Fortune 500 CIOs for IT acquisition (NEN, n.d.). A segment approach refers to the strategic allocation of IT services, functions, tools, and roles and responsibilities associated with end-to-end service delivery. DON officials selected this approach on the basis that it would provide increased flexibility in meeting NGEN capabilities and goals with no additional cost (GAO, 2011).

GAO officials’ evaluation of the segmented approach revealed increased risks of delivering components of IT services through multiple contracts. GAO officials maintain that the risks stem from the deficient AoA, which did not include risk evaluations associated with the segmented approach. The most egregious flaw determined by the GAO report was that the approach currently being pursued by DON was not one of the alternatives assessed in the AoA (GAO, 2011).

In the subsequent GAO report (2012) the program was flagged as a “high risk” due to the lack of defined roles and relationships among segments and government functions. The apparent lacks of defined seam management will increase the level of risk and will be detrimental to the life cycle development and implementation of NGEN.

D. CONCLUSION

GAO officials reviewed the intended ETAs and contracts and concluded that the acquisition decisions were not always performance or risk based. DoD, DON and OSD officials felt they had sufficiently mitigated known risks and issues and had advanced the program in spite of the apparent shortfalls and risks. The entire program was plagued by a lack of defined requirements, time constraints, and inadequate analysis of alternatives but was always approved at a key acquisition review. Risks identified in the past materialized into critical issues that have stagnated the transition efforts and added several billions of dollars to the estimated cost at completion.

IV. NGEN AND NMCI: THE COMMON GROUND

"Those who cannot remember the past are condemned to repeat it."
—Philosopher George Santayana

A. INTRODUCTION

When the DON was implementing NMCI, a study done by the Standish Group[18] International revealed that out of 7,400 IT implementation projects evaluated, 34% were late or over budget, 31% abandoned, scaled back or modified, and only 24% were completed on time and on budget (Cunningham, 1999). In 2005, in a report published by the Klynveld Peat Marwick Goerdeler Consulting Firm[19] of IT implementation across 600 organizations in 22 countries found that within a 12-month period, 49% of organizations had suffered a recent project failure with only 2% of organizations reporting success in achieving desired benefits. In 2008, OMB painted an equally bleak picture of the state of over 400 federal government IT projects; with over $25.2 billion in expenditures for fiscal year 2008, the projects were listed as poorly planned, poorly performing or both (GAO, 2008).

For all the reasons that lead to failures in implementing IT, many experts agree that poor management of organizational change is the key contributor to incomplete or otherwise unsuccessful IT implementations (Gibson, 2003; Umble & Umble, 2003). This poor management can manifest in inadequate planning of management activities and controls, especially a lack of single-point accountability for deliverables, resulting in the project failing to meet its objectives (Fuerst & Cheney, 1982). Others believe success in IT projects cannot be defined only in terms of achieving time, cost and quality objectives, but must also have the objective of meeting stakeholders' expectations, in particular, the client/user. Therefore, managing the expectations of stakeholders is a critical

[18] The Standish Group is an IT research-focused organization based in Boston, MA. It is a premier IT leader in project and value performance with dedicated professionals with years of practical experience in assessing risk, cost, return and value IT investments.

[19] Renamed BearingPoint on October 2, 2002, Klynveld Peat Marwick Goerdeler (KPMG) is one of the largest professional services firms spun off the consulting unit of KMPG as KPMG Consulting, LLC.

management strategy that should be treated with urgency (Bryson, 2004; Bennatan, 2002). Failure is also attributed to unrealistic, incomplete, and dynamic requirements, and some experts argue that it is increasingly urgent to specify requirements in order to utilize IT resources effectively within a project's timescale (Ward & Elvin, 1999; Baccarini, Salm & Love, 2004). Other failure causes include technology and technical issues, unpredictable external factors, political circumstances, and politically motivated requests embedded in the project, which become difficult to manage and meet objectives. Sometimes the projects are not viable due to economic circumstances, and unpredictable human behavior may also sabotage a project.

This chapter cannot address all the reasons that contribute to the failures of implementing IT in complex organizations. However, it will attempt to address the underlying issues with implementation of stakeholder management, requirements, and personnel management that plagued the implementation of NMCI and continue to plague the transition to NGEN. The analyses in this chapter will be done using a variation of the Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis template. The basic SWOT described by the originator Albert Humphrey, was a derivative of research conducted to by the Stanford Research institute to evaluate change management in organizations (SRI, 2005). Current use SWOT analysis is primarily structured as planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats of decision based objectives for new ventures in organizations. For this chapter SWOT will be used retroactively to assess previous IT implementation strengths and weaknesses. The SWOT analysis will also recommend future opportunities assessing internal and external conditions have influence on achieving the successful implementation of NGEN

This chapter will recommend holistic change management practices that take into account the various stakeholders and the change process and leverage on key interdependencies. The application of a more robust model that aligns resources and activities and provides means to identify critical paths can provide a testable model applicable to all phases of IT change in United States government.

B. FAILURES IN IMPLEMENTING IT

1. Stakeholders Expectation

Freeman (1984) defines any group or individual who can affect or is affected by the achievement of the organization's objectives as stakeholders. More detailed definitions from Kanter, Stein, & Jick (1992) ascribe the group responsible for identifying the need for change, creating a vision and specifying a desired outcome, and then making it happen as change agents, and the group responsible for implementing, adopting, or adapting to the change as the change recipients. Hannon (2004) further defines the group by three relationship attributes of power, legitimacy, and urgency. Figure 6 captures the qualitative classes of stakeholders, the nature of the relationship attributes, and the overlaps that might be present when seeking to identify relevant stakeholders. The stakeholders are classified as the groups with the ability to influence the organization; those with legitimacy and that are vital to the organization, and those with a claim that demands immediate attention. For the purpose of this paper, the term “stakeholder” is used to capture all the groups that induce change and the groups that receive and respond to elements of change in an organization.

The challenge of the different stakeholder groups is the disparity in expectations resulting from the required negotiation and appeasement of all stakeholders with the intent of achieving a common ground to pursue the project goals and maintain the project management effort. Further exacerbating the already daunting challenge is the manner in which the stakeholders view the level of their power and influence on the project. Stakeholders view their role in a project differently based on socially constructed realities forged and enforced by multiple perceptions of the members of each stakeholder group (Hannon, 2004). Hannon (2004) further argues that for a project to be successful, the stakeholders’ criteria of satisfaction have to be met.

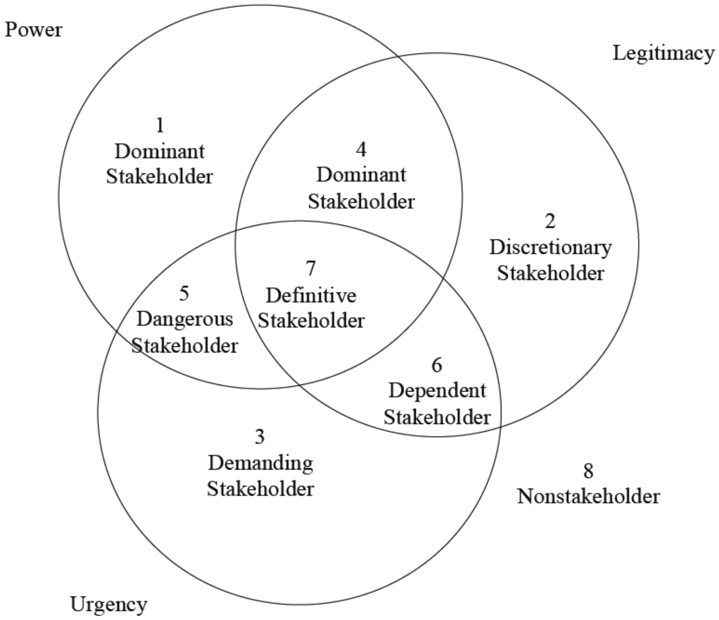


Figure 6. Qualitative Classes of Stakeholders (After Mitchell, Agle & Wood, 1997).

The main stakeholders associated with the change from the disparate networks to NMCI included the legislative branch of the government, senior naval officials, the end-users, and the vendors (external service contracts). The struggles of the NMCI implementation have been discussed in prior chapters, but when subjected to stakeholder analysis, the predominant perception is one that reveals a chasm; stakeholders imposing the change and stakeholders affected by the change.

For NGEN, the stakeholders are very much same as NMCI's though senior naval officials have reserved the option to outsource to multiple agencies for the transition of the network. DON intends to use multiple vendors to provide the planned segmented approach for NGEN capabilities. The intent of a multiple-vendor approach is to mitigate excessive financial cost to the government by vendor competition, and, as a secondary consequence, improve the services provided for NGEN. This measure could possibly displace HP as the primary facilitator of the network and add more vendors.

a. Strengths

In the indelible words of the U.S. Constitution, the legislative arm of the government is "To raise and support Armies … and to provide and maintain a Navy" (U.S. Const. art. I, § 8). The expectation for the past 237 years has been that as the only governing authority that can appropriate taxpayers' dollars, Congress disburses funds to the DoD through the annual Defense Appropriations Act to support and maintain defense operations. The DoD in turn is accountable to Congress and responsible for reporting on all funding allocated to activities within the departments. The reciprocity of the relationship between the legislative branch and DoD ensures checks and balances in a complex environment, and that stakeholder interests (i.e., the common defense of the homeland) are upheld.

Today, DoD is one of the largest and most complex organizations in the world, with operations consisting of over $1.8 trillion in assets, $2.2 trillion in liabilities, and over 3.2 million military and civilian personnel with annual disbursements of over $947 billion (GAO, 2010). To cope with its size and complexity, DoD has developed and continues to add to a vast library of instructions and directives that govern its personnel and their execution of policies, resources and requirements, acquisitions, and fleet readiness to include support and field operations. Instructions and directives such as the Naval Military Personnel Manual explicitly define the nature of interactions amongst members of DoD, setting a baseline expectation and providing structure and uniformity.

In spite of the large number of military and civilian personnel within DoD, the department does not have employees in sufficient numbers with all the skills to meet every requirement, and it has to award external service contracts (vendors), which are essential for carrying out the myriad of functions required by DoD (GAO, 1991). As with DoD members, there are instructions that set the baseline level of expectations for all recipients of external service contracts. One of the documents that set the level of expectation for contractors and vendors is the RFP, which is mandated by the Federal

Acquisition Regulations (FAR).[20] The RFP is a formal solicitation used in negotiated acquisition to communicate government requirements to prospective vendors and to solicit proposals (FAR 15.203). A properly written RFP will contain elements such as the statement of work, which describes what services the government wants supplied and the nature and scope of the tasks being requested. It also defines the nature of the relationship; how the government contracting officer and the vendor will interact, how information will be exchanged administratively, and the terms of payments (usually tied to expectations of performance and delivery of services).

The U.S. government has sought to eliminate speculation from all of its overarching activities and processes by providing baseline guidelines and instructions. The result is a visible and dependable structure of operations where there is an explicit understanding of the expectations and requirements for its members and service contractors. On the macro level, the government has the right mechanisms in place to address its stakeholders and this can be seen on the micro levels with formation of working groups such as the NGEN System Program Office (SPO). The Chief of Naval Operations and the Commandant of the Marine Corps approved the NGEN SPO, a first-of-its-kind organization in the DON, because it sought to bring relevant stakeholders (i.e., policy, resources and requirements, acquisition, and fleet readiness, support and operations) under a single command (Riley, 2008). Top Navy officials understood that each stakeholder had different interests, different expectations as to the results of the project, and different definitions of when the project would be deemed successful. So to facilitate a smooth transition to NGEN from NMCI with no loss of services to end users, Navy officials provided a medium through NGEN SPO to voice and foster a new level of coordination between all stakeholders in the implementation of the NGEN initiative.

[20] The Federal Acquisition Regulations (FAR) is the primary regulation for use by all Federal Executive agencies in their acquisition of supplies and services with appropriated funds. It became effective on April 1, 1984, and is issued within applicable laws under the joint authorities of the Administrator of General Services, the Secretary of Defense, and the Administrator for the National Aeronautics and Space Administration, under the broad policy guidelines of the Administrator, Office of Federal Procurement Policy, Office of Management and Budget.

b. Weaknesses

The challenge with stakeholder expectations is the disparity in expectations, and the more stakeholders in a complex environment such as the DoD, the greater the existence of multiple environmental elements with diverse intentions, demands, and expectations (Hannon, 2004). A medium to facilitate total stakeholder disclosure and subsequent negotiation of the diverse stakeholder expectations should be the norm and not the exception, but often, as seen in implementation with NMCI, such a medium was nonexistent. The absence of open communication to collaborate and discuss expectations by the relevant stakeholders creates void or false expectations, which results in disillusionment and a decrease in the credibility of the project (Taylor, 2006). The lack of communication is not always the cause of the stakeholder interaction, but sometimes it is the effect of the interaction. A recent hearing before Congress concerning challenges to vendors doing business with the DoD, revealed the trend of more vendors being unaware of what their clients might need and an increased reluctance to share their ideas. The reluctance stems from concern that ideas discussed will be compromised because the vendors might no longer have the differentiator that wins the next award (U.S. House, 2010).

The lack of disclosure in stakeholder communication can lead to false expectations and a decrease in the credibility of the project; conversely, taking into consideration the different criteria of satisfaction and viewing each as a goal to be met can lead to a compromised end product. Shillabeer, Buss, & Rousseau (2011) claim the nature of the process of negotiating is inherently flawed because it ensures the end product is unlikely to fulfill every stakeholder’s expectation.

The GAO report (2006) claimed that after six years and $3.7 billion, the NMCI program had not met the expectations of the intranet. GAO cited the failure to achieve information superiority and collaboration through interoperability and shared services as a blatant departure from the stated strategic goals of the intranet. It further attributed this deficiency to Navy leadership’s failure to implement a viable plan to monitor how these goals were being met. The failure was as a result of the desultory planning that plagued the intranet from its inception, but it was also a result of fallacious expectations by the stakeholders, leading to a compromised end product.

Congress has expectations that all MAIS[21] procurements by the DoD would be facilitated through the established acquisition procedures and without deviation from the law except with proper authorization. Consequently, as Navy officials attempted to bypass the traditional procurement process by labeling NMCI as a "service" and not a "system," Congress became militant toward every initiative with the nascent intranet and almost eliminated the program altogether (Taylor, 2006). Navy officials also suffered disillusionment in regards to expectations for NMCI as the projected pace of implementation continued to slow down. The impediment was due to a halfhearted accounting of legacy systems and subsequent software compatibility problems with the newly installed NMCI machines. Navy leadership expected due diligence in the accounting of the disparate systems by Echelon II commands; they also expected the same commanders to communicate the urgency of the network, but were disappointed on both accounts.

EDS received the direct consequences of failed expectations. By early 2003, EDS had invested nearly $2 billion in the project with the intent to recoup any losses further down range when the capital costs were minimal. This plan was thwarted due to the lengthy delays caused by the legacy application problem, and the slower-than-planned seat delivery rate greatly affected its NMCI business model and would cost EDS $3 billion. The end users for whom the system was designed never had any input. Taylor (2006) argues that the most important stakeholders in the NMCI program were the end users, but they were never involved in the decision-making, so there was no buy-in. The end users in general appeared to be ill informed about what it would take to be part of the NMCI enterprise and this ignorance caused the end users to be either apathetic or blatantly resistant. The apathy manifested in the benign forms of frustration, but the more

[21] Designation for all systems of computer hardware, computer software, data and/or telecommunications that perform functions such as collecting, processing, storing, transmitting and displaying information, which exceed $378 million (FY 2000 constant dollars) for all expenditures, for all increments, regardless of appropriation or fund source, directly related to the AIS definition, design, development, deployment, operations and maintenance, and incurred from the beginning of the MSA phase through sustainment for the estimated useful life of the system

adept user with "autonomous" control of a legacy system(s) would experience a rude awakening when transitioning from localized control to a high degree of centralized control and operation. The belligerent end user would often make deliberate attempts to antagonize EDS's efforts during local installation.

The expectation for NMCI was highly ambitious at best and not shared by all the stakeholders. The expectation of what NMCI could be and what it would provide generated anticipation and promise, but the mismanagement of this expectation and the consequent friction it generated led to lost time, capability, and money. To the credit of all the stakeholders, there were always attempts to salvage NMCI and steer it back on track, but the end product fell short of the initial design. Gutierrez & Friedman (2005) see the process of realignment and redesign as a way to compensate for certain elements of a project considered to be the cause of a current and less desirable state, but often the compensatory action just does enough to satisfy the basics of the original requirements. Figure 11 shows the cascading nature of expectations and the stages that the stakeholders experience after realizing that the gap between the vision and the current reality is greater than anticipated.

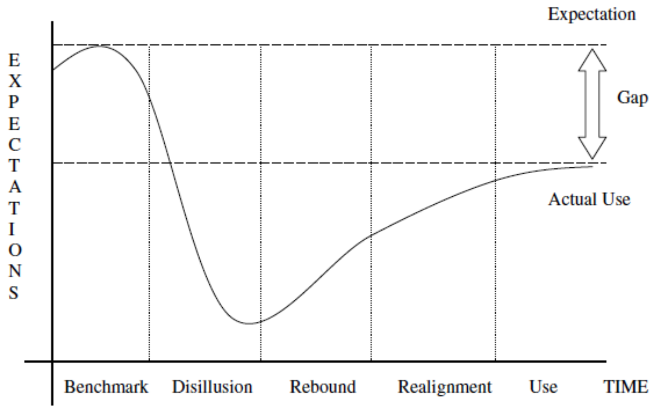


Figure 7. Project Management Cycle **(**From Gutierrez & Friedman, 2005).

Peter Senge, in *the fifth discipline: The art and practice of the learning organization*, claims that there two ways to respond to a gap between the current state and the vision. The first is known as a "fundamental solution" which takes proactive action to bring reality in line with the vision; the second is the “symptomatic solution” which seeks to lower the vision to bring it in line with the current reality (p.152). The Navy’s vision for NMCI was to consolidate the 1,000 diverse legacy systems and shore-based networks (all operated and maintained by separate organizations and vulnerable to intruders). The NMCI benchmark envisioned by the Navy leadership promised rapid and seamless communication, collaboration, and data exchange with anyone on the network, but the implementation of the intranet would confirm the words of German military strategist Helmuth von Moltke, “No plan survives contact with the enemy” (Two guys meet, 2013). The enemy would include haphazard accounting of legacy systems, incompatibility of software, end user resistance, and hostility from Congress. The consequent disillusionment and attempt at realignment would force the Navy to lessen its vision to keep the contractor “well” by contract extensions and a reduction of the number of SLAs used to evaluate performance, and the decision to begin paying for legacy system support (Taylor, 2006)

Today, NMCI provides about 382,000 workstations to approximately 700,000 users across 2,500 Navy and marine corps locations around the world, facilitating the transfer of over 3.5 terabytes of data while denying in excess of 2 million unauthorized access attempts and disinfecting tens of thousands of viruses (DoD, 2009; GAO, 2011). The capability of NMCI today is adequate to satisfy the core of the original requirements, but the reality is that the current environment is a compromise of what it could have been. With costs to run the NMCI network at about $1.2 billion a year, in addition to the $1.5 billion required to run the legacy networks (permitted to continue operations as “excepted” networks, albeit with a lack of the much needed interoperability and standardization), it seems the Navy leadership settled with the same problem it had in the beginning (Taylor, 2008).

c. Opportunities

One of the ETAs being used to facilitate the smooth transition from NMCI to NGEN is the Global NetOps command and control Workforce Establishment (ETA 1C). NGEN requirements document (2008a) identified a gap in the number of personnel with the degree of competency in technical and process maturity capability required for the daily operations of NGEN. The ETA will ensure the government is ready to assume oversight in a government-owned and networked environment, given its size and complexity. ETA 1C provides enterprise-wide position descriptions and occupational standards for standardized training, advancement criteria, and performance objectives based on DoDD 8570.01M, the premier document for guidance on DoD information assurance training, certification, and workforce management.

DoDD 8570.1M (2007) identifies and categorizes positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD GIG in accordance with overarching DoD directives.[22] The requirement for an adequate workforce began as a phased approach in 2005, and after its fourth year it mandates that all IT initiatives must be in 100% compliance with 8570.1M, further specifying that the Department of Defense requires approximately 110,000 identified IA professionals to be certified. In order to assure that the NGEN Workforce is DoD 8570 1 compliant, DON leadership plans to conduct a job task analysis and assess learning tools for contractor technical representatives to develop enterprise-wide position descriptions and occupational standards for training, advancement, criteria, and performance objectives (GAO, 2011).

Though this ETA is essential to develop standards for training, advancement, criteria, and performance objectives, it does little to address the dynamic of the stakeholders' expectations in light of the seemingly increasing complexity of NGEN. The Navy leadership needs to ensure all relevant stakeholders have a grasp on what is expected.

(1) Share the Vision

With the influx of over 100,000 professionals identified by the DoD for IA purposes, DoD is in the prime position to imbue its nascent members with a consolidated strategic vision of the net-centric environment it strives for. The opportunity to leverage lessons learned from the consolidation of the disparate networks is

[22] DoD Directive DoDD8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002 and DoD Directive 8500.1, "Information Assurance," October 24, 2002

immeasurable, considering the many missteps that plagued the NMCI project. With NMCI, Taylor (2006) acknowledges the existence of a vision for the intranet, but contends the vision was not accepted by the organization because the main stakeholders, including Congress, the Navy's executives, and most importantly, the end users, did not fully understand why NMCI was important and why it needed to be implemented as soon as possible (pp. 8283). Brynjolfsson, Renshaw, & Alstyne, (1997) discovered from a survey a high variance in stakeholder priorities, and they attribute the variance to a fragmented vision. Brynjolfsson et al. further contend stakeholders with different priorities will tend to work at cross-purposes during implementation, and the act of genuinely soliciting input gives stakeholders a sense of ownership and responsibility, which has a positive effect on the change process.

The idea of having "all" stakeholders' inputs not only ensures a buy-in to the idea for all parties concerned, but it also ensures that the vision is shared. Westley & Mintzberg (1989) claim that a "vision comes alive only when it is shared" because the dynamic relationship rather than the unidirectional norm, is the key to motivating people to coalesce and realize a desired vision. A dynamic and reciprocal relationship is feasible in most employment environments because of informal, less-structured leader-follower arrangements, but for organizations that require a stark distinction between leaders and followers, such as the military, the unidirectional vision from the top down is a staple (Gardner, 1987, p. 187). Taylor (2006) highlights the overt decision to exclude Congress and the failure to include the end user in the implementation of NMCI as a critical failure on the part of the Navy leadership. Goss, Pascale & Athos (1998) echo the sentiment because the end users have strength in numbers; therefore, for a transformation effort to be successful, it

> …must encompass a critical mass of stakeholders – the employees "who really make things happen around here." Some hold sway over key resources. Others are central to informal opinion networks. The group may often include critical but seldom seen people like key technologists and leading process engineers. The goal is a flywheel effect, where enough key players get involved and enrolled that it creates momentum to carry the process forward. (Goss et al., p. 102)

The vision from the Navy leaders had to be shared by all the stakeholders because a shared concept becomes a “shared covenant that bonds together leader and follower in a moral commitment” (Sergiovanni, 1990). Murphy (1988) further stresses the importance of a shared vision because it “is rare to see a clearly defined vision articulated by a leader at the top of the hierarchy and then installed by followers”. Sharing the vision is exceedingly difficult to implement across the entire breadth of an organization such as the military due to the sheer size and the complexity of the organization’s daily operations. This difficulty lends to the argument against a shared vision, the essence of collaboration, which often can be lethargic and a singular impediment to urgent needs for change or demands for quick action. The negatives to not sharing a vision with every stakeholder can also be detrimental to the process as evidenced in the pitfalls of NMCI implementation. Navy and Marine Corps leaders made the right step with the formation of NGEN SPO working groups (Riley, 2008). Instead of disestablishing the NGEN SPO, it should be continued and be all-inclusive of all the stakeholders especially as the segmented network will be supplied by multiple vendors.

d. Threats

Many threats that still loom over the implementation of NGEN are residual from the efforts of implementing NMCI, but most of the threats are unique to the NGEN experience. The GAO (2011) report claims the acquisition approach that DON intended for the implementation of NGEN was not one of the alternatives assessed in the analysis, and it was potentially riskier and costlier than the other alternatives analyzed because of the higher number of contractual relationships (GAO, 2011, p1). As the discussed in earlier chapters, DON officials contend the segmented approach was selected because of the increased flexibility in meeting NGEN capabilities and goals with lower costs than NMCI. This segmentation extends to the management domains of the network, where the USN will operate its own domain as a government-owned contractor-operated network while the Marine Corps will operate, as a government-owned government-operated network. The Marine Corps will primarily act as its own service provider with supplemental contractor support as needed. The different operational models are intended to allow the USN and Marine Corps to operate their respective domains in the manner best suited to support their different mission needs (GAO, 2012, p. 4).

The risk of segmentation as identified by the GAO (2011) report is the increase in the number of contractual relationships required to effectively implement and operate NGEN. The risk of the increase in contractual relationships is further compounded by the apparent lack of a plan for DON to facilitate coordination among contractors and the government in operating NGEN (GAO, 2012, 21). The threat of adding more contractual relationships to an already complex environment is that

> environmental diversity increases as the number of spheres of influence increases. A diverse environment may cause the work on one product to hinder the work on other products; services rendered to one type of customer may detract from the services provided to other types of customers. Organizational managers must be aware of their organization's environmental diversity. (Hannon, 2004, p. 18)

This diverse environment has seen focus on one product hinder the work on other products as more effort and focus was directed to additional planning before issuing the transport and enterprise services request for proposals and addressing industry comments on the draft request for proposals to prevent bid protests further down range (GAO, 2012, 18). This further planning consequently compressed the timeline and exacerbated the risks with NGEN implementation to include "potential delays in transition from the incumbent to the new service provider(s) and in contract award for the transport and enterprise services, as well as the potential lack of coordination among contractors and the government in operating the network" (GAO, 2012, p. 20).

Table 2. NGEN Program Critical Risks, as of July 2012 (After GAO 2012a)

Program identified critical risk	Program risk description from program documentation	Program identified risk level
Seam management	Roles and relationships among segments and government functions have not been defined or agreed on. If these seams are not accurately identified and characterized, DON will not be able to manage them effectively and the transition will take longer.	High

The GAO has made the point repeatedly of DON officials not doing a thorough and effective AoA, but DON officials have stayed the course and still plan to pursue the segmented approach amidst the ambiguity of touted flexibility using the chosen alternatives (GAO, 2011, p19). DON officials have deferred to the ETAs as adequate measures to establish government management capabilities, which will facilitate collaboration and accelerate the transition time (GAO, 2012, p12). The efficacy of the network depends greatly on the ability of DON to manage the relationship between different contractors and government elements. DON also has to ensure that the components that make up segments (an allocation of IT services, functions, tools, and roles and responsibilities associated with end-to-end service delivery) are compatible (GAO, 2012).

2. Requirements

Defining requirements for an information technology project is an extremely important, if not the most important, element for any successful project. Because IT projects are inherently complex, implementations require a meticulous requirements' definition process that stems from a shared vision. The shared vision refers to one that is built by all stakeholders and captures all relevant processes and activities. If the requirements are not clearly stated upfront, complexity is adversely affected and can exponentially increase the scope, cost, and the time of the overall project. The issue with requirements can be as basic as insufficient information from the customer, unrealistic expectations upfront, or a stated requirement that fails to meet the desired project objectives. Insufficient information is often a result of the ignorance of the customer, for example, the unknown unknowns,[23] and ignorance of the customer is usually a byproduct of taking on novel projects with immature systems or components. Being ignorant of the unknowns also negates the ability to plan and provide adequate contingencies against future risks. If there is a requirement deficiency, especially in the analysis phase, it will almost always lead to cost and schedule overruns in information system projects (Shand, 1994; Engming and Hsieh, 1994).

The federal government recognizes the negative impacts of not addressing its IT issue concerning requirements, and to that end has made great strides to mitigate the risks. The federal government, with the help of industry leaders, has collaborated to establish policy along with appropriate governance to ensure the effective application and evolution of IT. Certain policies have had positive results, while others, such as the LPTA mandate, have further hampered the issue with requirements. The dependence of the federal government will continue, but so will the complexity of the new interconnected global environment, and due diligence has to be given to the criticality of information technology.

a. Strengths

In a direct response to the findings of a congressional inquiry into the lack of proper management and oversight of IT in the federal agencies, Congress passed the Information Technology Management Reform Act of 1996 (Gillam, 2010). The reform act, later renamed the Clinger-Cohen Act after Rep. William Clinger and Sen. William Cohen who pushed the legislation through, would attempt to curb the numerous IT issues with acquisition regulations and IT management in the federal government. The Act realigned responsibility of agencies involved in the procurement of federal government

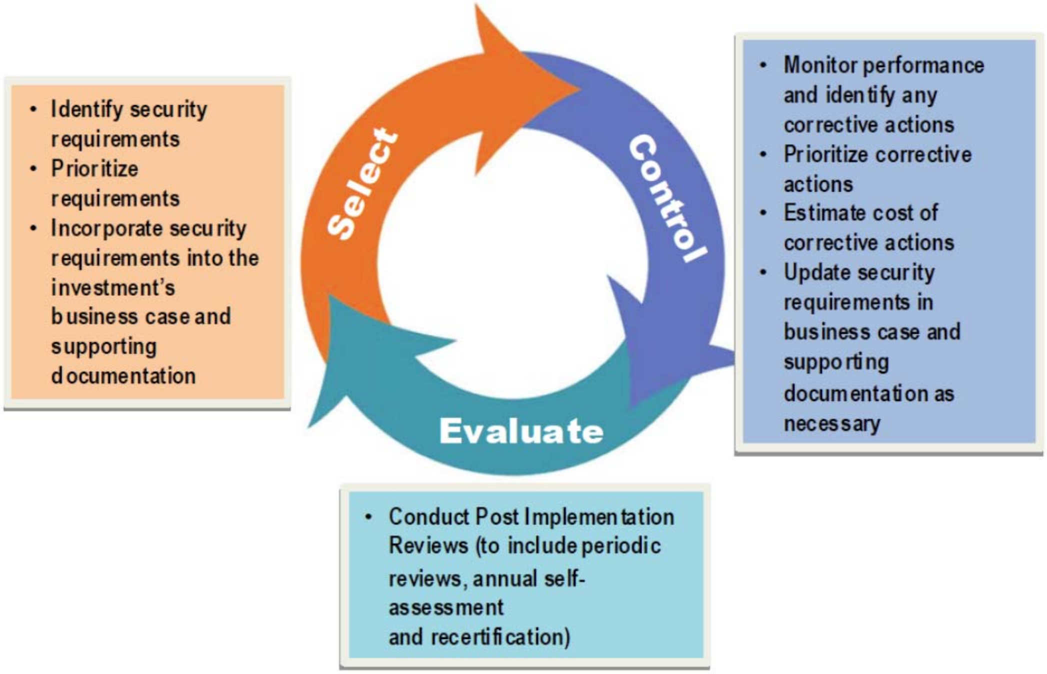
[23] United States secretary of defense, Donald Rumsfeld, during a DoD news briefing concerning issues with Iraq stated, “There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say, we know there are some things we do not know. But there are also unknown unknowns – the ones we don’t know we don’t know” Retrieved December 11, 2012 http://www.defense.gov/transcripts/transcript.aspx?transcriptid=2636

IT equipment and systems and established the position of CIO. Table 3 gives a summary of changes made by passing the CCA.

Table 3. Summary of Clinger-Cohen Act of 1996, Title 40 from National Defense Authorization Act for Fiscal Year (After Clinger-Cohen Act of 1996).

The law gives Office of Management Budget (OMB) responsibility for:
• Developing a process for analyzing, tracking, and evaluating the risks and results of major capital investments • Directing executive agencies on establishing an effective, efficient IT capital planning and investment review process, and enforcing accountability through the budget process.
The law gives executive agencies responsibility for:
• Establishing an IT capital planning and investment review process • Using performance measures to assess how well IT supports programs • Justifying continuation of systems that deviate from cost, performance, or schedule goals
The Clinger-Cohen Act establishes a Chief information officer (CIO) in executive agencies who:
• Reports directly to the agency head • Has Information Resources Management (IRM) as the primary duty • Provides advice and assistance to the agency head on IT and information resources management • Develops an integrated IT architecture • Promotes efficient and effective design and operation of IRM processes • Uses performance measures to monitor IT programs • Assesses the knowledge and skills of IRM personnel • Shares with the CFO responsibility for provision of financial and performance data for financial statements • Assumes the responsibilities of the Designated Senior Official defined in Paperwork Reduction Act

The CCA also provides guidance on the minimum required standards necessary for the effective operations or security of federal information systems and requires that federal agencies to use a disciplined capital planning and investment control (CPIC) process to acquire, use, maintain, and dispose of information technology (NIST, 2009). The CPIC process ensures all federal government investments in IT are made by integrating, budget, financial, and program management decisions to fulfill its missions and business needs. The CPIC accomplishes these requirements through three distinct phases (see Figure 8): select, control, and evaluate. The CPIC process is intended to be recursive and is essential to ensure that IT investments are effective. The recursive nature of the CPIC process allows evaluations (on quantifiable measurements) to be used to assess the risk and benefits of current investment issues, which provides senior management with concurrent information in regard to cost, timeliness, and quality.



Identify security requirements
Prioritize requirements
Incorporate security requirements into the investment's business case and supporting documentation
Select
Control
Evaluate
Monitor performance and identify any corrective actions
Prioritize corrective actions
Estimate cost of corrective actions
Update security requirements in business case and supporting documentation as necessary
Conduct Post Implementation Reviews (to include periodic reviews, annual self-assessment and recertification)

Figure 8. CPIC Process (From NIST, 2009, p.9)

The federal government also uses IT acquisition best practices utilized by private industries. Carnegie Mellon Software Engineering Institute[24] is one such industry that has established highly regarded and widely used guidance used by the federal government. The institute's Capability Maturity Model® Integration for Development aids the requirement creation process by initiating and managing products and services that include all supplier and acquirer activity. The model also seeks to eliminate some barriers by using common language to aid in requirements development and management, risk management, configuration management, validation and verification, and project monitoring and control.

[24] The Carnegie Melon Software Engineering Institute works closely with DoD and other government organizations, continually improving software with the goal of improving software engineering capabilities and developing or acquiring the right software, defect free, within budget, and on time every time.

GAO’s own research in IT management best practices and knowledge gleaned from past experiences with implementation of IT in the federal government led to the development of the Information Technology Investment Management Framework (GAO, 2011b). This framework was developed using the select/control/evaluate approach from the Clinger-Cohen Act of 1996 (see Table 3). The management framework also stresses critical oversight of system development and acquisition management, and organizes past performances and experiences into a set of critical processes for successful investments.

The federal government recognizes that IT is a critical resource and has thus spearheaded numerous regulations and directives along with appropriate governance to ensure the effective application and evolution of IT. The dependence of the federal government on IT will only continue to grow as more of its functions become automated and digitized to improve performance.

b. Weaknesses

GAO report (2011) contend one of the main weaknesses facing federal IT investments is requirements management because of its negative impact, such as cost increases and schedule delays, and in worst case, cancellation or significant restructuring (p.5). In regard to the implementation of NMCI, Jordan et al (2007) study revealed that DON did not define all of its technical requirements when it solicited contractor bids, and many of the critical technical requirements were not dealt with until after contract award. The most important failure for the lack of substantive requirement definitions would be the upgrade of legacy applications to meet the requirements for inclusion in NMCI. The flawed requirements management stemmed from the inception of the intranet idea because DON leadership had failed to develop a formal analysis of program alternatives and complete a business case analysis to determine an appropriate acquisition strategy for the proposed intranet. The AoA ensures the system or components being procured have been verified and validated through stringent MOE, cost, schedule, concepts of operations, and overall risk assessment. More importantly, the sensitivity of each alternative to possible changes in key assumptions or variables is determined.

The verification of the system answers the question, “Are we building the product right?” while validation testing answers the question, “Are we building the right product?” Properly performing an AoA can aid in ensuring that requirements are carefully developed and reliability guaranteed for the end product. Conversely, not following established procedures such as the AoA could affect a project negatively. For example, with NMCI the Navy leaders found that the number of legacy applications had substantially been underestimated, and this underestimation contributed to the transition period slipping from 2½ years to 3½ years (GAO, 2003). The GAO (2003) report claims the Navy and the Marine Corps did not perform a thorough analysis but instead performed an analysis at remote locations to obtain a baseline. This baseline did not include an assessment of the DON’s legacy applications since project officials decided to rely on outdated inventories (p. 36). The weakness described is clearly one of neglecting set directives designed to safeguard against the malfeasance of senior officials, but other issues are simply a consequence of the complexity of the federal government IT implementation.

Some weaknesses in developing requirements are due to imposed legislation, as was the case with NMCI where Navy leadership claimed that delays with implementation was due to the onerous certification and accreditation requirements for all applications and legislation requiring certain analyses to be completed before seat deployment could exceed specific levels. With NMCI, the requirements came in the form of SLAs laden with complex criteria, which ended up as a financial burden for EDS (Jordan 2007). Many contractors experience the dynamic nature of requirements, especially during the course of a solicitation where federal agencies such as the DoD will often change the requirements with very little time for contractors to respond (U.S. House, 2012).

These changes to requirements are usually a consequence of the lack of a thorough AoA at the genesis of a project, but can cause widespread reworking and rebaselining. Rebaselining is the issuing of a new revised baseline, estimate, and schedule because of new complexities and findings with a project; the “symptomatic solution” which seeks to lower the vision to bring it in line with the current reality. GAO officials reported that the key reasons for the most recent rebaselinings in government IT projects were changes in project requirements, objectives, or scope, and changes in funding stream. Table 4 shows the estimated frequencies of each of these reasons.

Table 4. Estimated Frequency of Reasons for the Most Recent Rebaselining of Projects Category of Reasons (After GAO 2008b)

Category of Reasons for the Most Recent Rebaselining of Projects	**Percentage of times reported**
Change in project requirements, objectives, or scope	55%
Change in funding stream	44%
Original baseline was inaccurate	14%
Cost or schedule overruns due to project performance	4%
Cost or schedule overruns due to contractor performance	4%
Other	41%

The changes are usually in response to an unexpected challenge and can be virtually non-ending. According to a study by Baccarini et al. (2004), the stakeholders' continuous changes to requirements are one of the highly ranked risks throughout the project lifecycle. The non-ending changes can also be attributed to the "cascading need effect," which is a byproduct of acquisitions of new information systems technology because it often leads to the acquisition of other support systems or the addition of unexpected tasks. This unexpected need or dependence on new information technology can cause an exponential increase to the overall cost and schedule (Benamati, Lederer, & Singh, 1998).

Until the relevant stakeholders have a comprehensive dialogue that fields input from all concerned, it will be difficult to have requirements that are sound and stable. Suppliers must fully understand what the customer wants so that limited research and development resources are invested effectively. The customer also has to involve all its stakeholders and leverage subject matter experts from industry to avoid pitfalls with requirement development. Without a comprehensive overhaul of the way requirements are developed, the result will be "overreach" on requirements, and an increase of cost, schedule, and performance problems in acquisition programs.

c. Opportunities

In the past, the federal government has leveraged the economies of scale and benefitted from the cost savings of large purchases, but when applied to IT systems the model is flawed. Economies of scale translate to acquiring system of systems, which can solve all problems, even those that are unknown. This approach is intrinsically flawed due to the complexity of IT and further exacerbated by the attempt to do too much at once given the complexity of the federal government. In the recent *25-point implementation plan to reform federal information technology management*, the U.S. CIO, Vivek Kundra, lamented on the dire state of information technology in the federal government. Kundra (2010) claims the federal government has spent over $600 billion on IT projects but has failed to deliver promised functionality because of its “grand design” approaches that deliver functionality every few years, rather than breaking projects into more manageable chunks and demanding new functionality every few quarters.

The idea of implementing IT in smaller “manageable chunks” refers to the method of building systems using an agile or modular development process. This process leverages an incremental, recursive, and collaborative process that is exhaustive and inclusive of all stakeholders. The idea is that instead of spending hundreds of millions of dollars on a mammoth system using a waterfall[25] approach, it might be better to break projects up into smaller elements with each element completely “certified” before advancing the project. One advantage of developing requirements with the agile/modular method is that it requires a greater cooperation and interaction amongst the relevant stakeholders. The service oriented architecture (SOA) 2008 working group, in a recommendation to DoD for acquisition of information services, suggested the agile and modular method to help the government rebalance the contractor SLAs because of the lack of interdependency not seen in the current environment (p. vi).

[25] The waterfall development model originates in the manufacturing and construction industries, highly structured physical environments in which after-the-fact changes are prohibitively costly, if not impossible. Since no formal software development methodologies existed at the time, this hardware-oriented model was simply adapted for software development. Retrieved from http://sunset.usc.edu/csse/TECHRPTS/1983/usccse83–501/usccse83–501.pdf

The benefits of the modular development are not a novel concept for the federal government and have been recommended in the *Federal Acquisition Regulation (FAR)* and the CCA of 1996. CCA recommends that "head(s) of an executive agency should, to the maximum extent practicable, use modular contracting for an acquisition of a major system of information technology" (Clinger-Cohen Act of 1996 § 5202). The FAR also endorses the use of modular development to reduce overall project risk and meet the federal government's need for timely access to rapidly changing technology. The question posed here is, "Why has the government not mandated the use of modular development in all of its IT implementation?" Or an even more pertinent question, "How can we verify that agencies are using modular development in IT implementation?" Though there is no one an answer to the questions, but the solution lies in a collective willingness to change the existing culture and leverage the available opportunities. Only then can the federal government avert the crisis of technology obsolescence.

The GAO Report *(2011) Better Informed Decision Making Needed on Navy's Next Generation Enterprise Network Acquisition* claimed NGEN capabilities, such as secure transport of voice and data, data storage, and e-mail, were to be incrementally acquired through multiple providers. The report, however, found though the first increment has been planned and budgeted for, future increments were yet to be defined. The report's further analysis used in determination of the increments was not reliable due to erroneous estimating methodology, rationale, and indiscernible results of a risk analysis (p. 12).

The complexity facing federal IT is critical, and the leadership must act now to mandate the use of modular development in all aspects of IT implementation and acquisition. Leveraging modular development and dividing IT investments into manageable elements has to permeate all relevant parties of the process. Modular methodology will ensure the project is verified and validated often in order to curb risks, while delivering much-needed capabilities faster. This methodology will prevent the federal government from fading into technological obsolescence, and, more importantly, allow for an all-encompassing effort in requirement development. The only caveat is that though it promises delivered functionality in shorter timeframes, is not one-size-fits-all and must be evaluated on a case-by-case basis.

d. Threats

GAO report (2012a) states that the entire NGEN program is currently plagued by a lack of defined requirements, time constraints, and inadequate analysis of alternatives, but it has been approved at a key acquisition reviews. The report also attributed the several billions added to the estimated cost at completion to risks identified in the past, which have now materialized into critical issues and stagnated the transition efforts. The issues with NGEN appear to be self-inflicted due to the desultory AoA done prior to the transition from NMCI, and these threats will continue with the choices DON leadership intends to follow through with.

One of the choices being made could result in an increase in the number of contractors and stakeholders, and its impact has been discussed as it pertains to stakeholder relationships. The increase in contractors has been lauded as a system to increase competition and decrease price, but it has raised new challenges in the area of collaboration. How will prospective contractors coordinate their various requirements for their segments? Are there any additional requirements for interoperability or security between the segments? The unknown elements associated with segmentation and the level of interoperability poses a clear and present danger, not only to the NGEN transition initiative, but also to the efficacy of organic net-centric warfare capabilities.

Another looming threat to requirements is cost. Threat of cost is precarious because on one hand the DON officials are trying to procure NGEN at the LPTA while abdicating the responsibility of doing a thorough assessment on alternatives. On the other hand, the vendors are trying to no avail to balance a triad of cost, quality, and profit. The idea of the LPTA process is appropriate when best value is expected a priori from a selection of technically acceptable proposals. The ideal, however, has not translated into practice and has served as an impediment to effective development of requirements and adoption of technology because it forces behavior that pretermits superior products to save on the price (U.S. House, 2011).

With cost as a driver for requirements, the federal government has painted itself into a corner and ensured that it is isolated from the best technology available. In his testimony before Congress, Hodgkins III, senior vice president for national security and procurement policy, TechAmerica, asserted his belief that the LPTA had nurtured an environment that deterred the pursuit of the best ideas and genuine innovation but encouraged competition that is based on the lowest offer from vendors that have met the minimum technological requirement (U.S. House, 2011).

For vendors that do meet the minimum technology requirement, small businesses are marginalized because they often "cannot achieve economic order quantities to reduce unit costs the way large companies can" ((U.S. House, 2012). To potentially repress the contribution of small businesses results in lost innovation and agility, and detracts from the idea of preserving a free competitive enterprise. The LPTA has evolved to value low price considerations over quality, so government personnel can expect inferior end products as the norm rather than the exception.

3. Management

There is no substitute for effective use of resources and time especially in large projects. Good management is indispensible at every level of organization, from garage start-ups to global conglomerates. The complexity of today's organizational climate commands that managers not only solve problems as they arise, but must also be proactive and prevent problems. This concept applies to project management where the manager is responsible for the planning, budgeting, execution, and closing. For each project, the number of interdependent elements varies and has to be identified and analyzed, a task not easily achieved in even the simplest of projects. Interdependencies can cause overt or covert disruptions that if not checked can cause major projects to fail.

Failure of major IT projects is the norm rather than the exception, and poor management is one of the main causes. Though a main cause for IT failure, the point of single-point accountability is moot when referring to colossal and complex systems such as NMCI and NGEN. In most large and complex organizations, the difficulties in managing any transformation are greatly increased and some experts agree that poor management of IT projects is the key contributor to incomplete or otherwise unsuccessful IT implementations (Gibson, 2003).

For successful IT implementation, a management cadre must receive the right support from the leadership, be competent for the level of responsibility assigned, and prioritize the requirements by understanding the present state and the desired end state of the project. Beckhard & Harris (1987) claim that not understanding the desired end state is the most significant threat to successful change management because its emphasis is on the desired termination point. Anderson & Anderson (2001) claim a clear and definitive goal or end state guides leaders to a planning process with greater certainty on how to get there, though the process can be challenging because of unforeseen complications and burdens. This challenge was clearly the evident during the installation of the new and centralized NMCI network, which was burdened with the extra task of migrating and merging the indispensable legacy systems (Taylor, 2006).

Understanding the present state in the case on NMCI was difficult because, according to the GAO report (2011a), the current state of NMCI before the decision to move to NGEN was not available or easily verifiable since the data was proprietary to the contractor. Without a proper analysis of the current state of NMCI, officials at the GAO have asked Congress to stop progress on NGEN. DON officials refute GAO’s claim and assert that several ETAs will facilitate a seamless transition between NMCI and NGEN and be sufficient to mitigate all risk. The ETAs have since been deemed ineffective in the GAO report (2011a) citing DON’s failure to conduct an accurate analysis of alternatives in the acquisition process, leaving decision makers without assurance that their selected approach is the most promising and cost-effective course of action.

Managing IT, either as a project such as a transition and implementation or as the daily maintenance and sustaining of a complex network, requires a high level of agility and competence from relevant managers. Managers must possess a comprehensive knowledge base augmented with vigorous training to effectively manage and balance the cost, performance, and schedule to ensure the government has the best bang for its buck.

a. Strengths

As discussed in previous sections, the government has a rigid hierarchical structure that has been essential to the common defense of the homeland. Also intrinsic to this environment is highly structured standards of operation. With the acquisition and implementation of MAIS, the management is governed by the MAIS acquisition lifecycle. The current MAIS acquisition lifecycle is derived from the five phases of the acquisition life cycle:

- Materiel Solution Analysis
- Technology Development
- Engineering and Manufacturing Development
- Production and Deployment
- Operations and Support

Though a very restricted sequence, program managers are expected to streamline this model to the maximum extent possible, consistent with technical risk, to provide new systems to the warfighter as quickly as possible (DAU, n.d.)

The management of MAIS in the DoD starts during the concept refinement portion of the pre-acquisitions phase with the charter of program managers (PM) and integrated project team (IPT). The program manager and IPT charter sets the tone on how the program will be managed. It identifies the roles (for government personnel and contractors) and responsibilities, and assigns liability to relevant stakeholders. With the designation of the PM and IPT, the team is expected to perform a comprehensive AoA, create am information assurance plan, and provide the first of three Clinger-Cohen compliance reports (see Table 3 for summary of the CCA of 1996). With a successful Milestone[26] review, the program can exit the pre-acquisition phase and enter the technology development phase.

The development phase is based on validation of the interoperability and supportability of the system being developed. The Levels of Information Systems

[26] All milestone reviews are by the Office of the Secretary of Defense (OSD) Investment Review Board (IRB), certified by the designated approval authority. The Defense Business System Management Committee (DBSMC) must approve the certification before any funds for modernization can be obligated.

Interoperability checklist guides the management through the development phase by identifying the different levels of complexity necessary for system-to-system information exchanges and provides a common DoD basis for requirements definition and for system improvements (DoD, 1998). In this phase the PM and IPT are required to develop the configuration management plans, the cost analysis requirements document, and the acquisition program baseline, and conduct the second Clinger-Cohen compliance report. Following a successful second milestone review, the program is allowed to exit the current phase and enter the following phase.

This activity continues for another three or four phases and involves the PM and IPT in a rigorous system requirement analysis, a software requirement analysis, an IA validation, system performance measurements and a Clinger-Cohen compliance report before the program is subjected to a milestone review. The management of the MAIS life cycle culminates in the full rate production and deployment, where management shifts from the sequential phases to operation performance oversight, punctuated with annual security reviews and tests.

The MAIS life cycle is a highly structured guideline for the PM and IPT to navigate the complex and length acquisition cycle of information systems. The strength of the MAIS lifecycle is the systematic flow of development and the consequent assessments by multidisciplinary groups such as the Investment Review Board and the Defense Business System Management Committee. These assessments allow for different perspectives on the same process and aid in detecting deficiencies that might be overlooked by a more homogeneous group.

b. Weaknesses

In the Challenges to Doing Business with the Department of Defense (2012), the high rate of personnel turnover of government acquisition personnel was seen as a management problem that led to failures in IT acquisition. The transient nature of DoD personnel due to the frequent PCSes pervades all areas of DoD, to include the Defense Contract Audit Agency (DCAA). The immediate consequence for an agency such as the DCAA is a break in continuity and consistency with regard to the application of acquisition policy. The report asserts the long-term implications appear even direr as a DCAA becomes more under-resourced and lacks trained, skilled personnel, hampering the ability of these agencies to provide appropriate contract oversight and management (p. Vii). The lack of skilled personnel, especially in the field of IT, in the government can be attributed to the long-held misconception by DoD leadership that employment of industry experts to manage the information systems would free warfighters to concentrate more on fighting wars (Taylor, 2006). This issue with management is not unique to the DoD organization as "many organizations are flat and lean, with many competencies outsourced, so it is not unexpected that personnel shortfalls are the highest ranked risk" (Baccarini et al., 2004, p. 290). In Challenges to doing business with the Department of Defense (2012), it was noted that DoD's reliance on private contractors could lead to a conflict of interest and blur the lines between work that must be done in-house and what work is permitted to be performed by private contractors (p. vi). Furthermore, with the NGEN transition, the issue of insufficient skilled personnel attributed to DON's failure to establish the sequence of activities with direct impact to the planned completion date of the transition to NGEN (GAO, 2012a, p. 9).

Other management weaknesses prevalent in the DoD have to do with its Command and Control management style. C2 in its simplest form is the unidirectional exercise of authority by a properly designated commander over assigned and attached forces in the accomplishment of the mission. This typical centralized command structure (depicted in Figure 13) affords its subordinates minimal feedback on how strategy is created by placing an emphasis on output over outcome (Shane, 2010, p. 11). Taylor (2006) describes the Navy's traditional strategy for introducing change as a "fast implementation with minimal communication and the end-user has no choice but to accept the change and move on" (p.111).

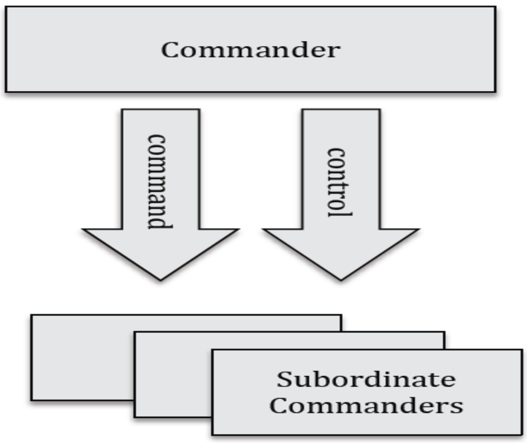


Figure 9. A Typical View of Command and Control—Command and Control Seen as Unidirectional (After MCDP 6, 1996)

Though the end user was forced to accept the changes, the “feedback” system in place was flawed. GAO (2006) report claimed a disparity in the reporting DON official’s submitted and the one done by GAO officials. The report claimed the Navy had not disclosed the range of performance measures and customer satisfaction issues. Though Navy officials refuted the claim stating the reports done were adequate as-is, GAO officials disagree. Without a meaningful feedback loop and Accurately disclosing program and contractor performance, and customer satisfaction to the relevant leadership then the issues and deficiencies will continue to linger.

c. Opportunities

In the 25-point implementation plan to reform federal information technology management, (2010), Kundra urges the federal government to leverage a well-developed program management talent strategy that will be the common denominator of high-performing IT organizations. DoD has made great strides already with its ETA to establish a Global NetOps Command and Control Workforce. The activity seeks to develop enterprise-wide position descriptions and occupational standards for standardized training, advancement criteria, and performance objectives in accordance with DoDD 8570.01-M the premier document for guidance on DoD Information Assurance Training, Certification, and Workforce Management.

DoD 8570.1-M (2007) identifies and categorizes positions and certification of personnel conducting IA functions within the DoD workforce supporting the DoD GIG in accordance with overarching DoD directives.[27] The requirement for adequate workforce began as a phased approach in 2005 and after its fourth year it mandates that all IT initiatives must be in 100% compliance with 8570.1M, further specifying that the Department of Defense requires approximately 110,000 identified Information Assurance professionals to be certified. Kundra (2010) contends that the management of federal government infrastructure must begin with the training and certification of personnel, but must be followed by provisions for lucrative career paths to attract and retain the very best performers in the IT industry.

In addition of adding competent personnel to the federal work forces, there must be open collaboration of multi-disciplinary teams with relevant skill sets before beginning major IT programs. GAO report (2011b) highlighted successful IT implementations based on their respective cost, schedule, scope, and performance goals. The common success factors were as follows:

- Program officials were actively engaged with stakeholders.
- Program staff had the necessary knowledge and skills.
- Senior department and agency executives supported the programs.
- End users and stakeholders were involved in the development of requirements.
- End users participated in testing of system functionality prior to formal end user acceptance.
- Government and contractor staffs were stable and consistent.
- Program staff prioritized requirements.
- Program officials maintained regular communication with the prime contractor.
- Programs received sufficient funding.

The report echoes the importance for a competent cadre of program managers; a group of consummate professionals that are just as knowledgeable as the

[27] DoD Directive 8000.1, “Management of DoD Information Resources and Information Technology,” February 27, 2002 and DoD Directive 8500.1, “Information Assurance,” October 24, 2002.

contractors. This team would be very beneficial because the customer and contractor would understand exactly what the requirement and proposal really means and avoid potential waste of resources.

In implementing IT, the government should process tasks required to satisfy each milestone decision by leveraging nine best practices for developing and maintaining a reliable schedule. In the GAO report (2011) *Better Informed Decision Making Needed on Navy's Next Generation Enterprise Network Acquisition*, the nine best practices recommended are as follows:

- Capturing all activities
- Sequencing all activities
- Assigning resources to all activities
- Establishing the duration of all activities
- Integrating schedule activities horizontally and vertically
- Establishing the critical path for all activities
- Identifying reasonable "float" between activities
- Conducting a schedule risk analysis
- Updating the schedule using logic and durations

These nine best practices ensure that a critical path is established and the chain of dependent activities is identified. Identifying the critical path is essential in complex projects because of the high level of interdependencies, which means that if any predecessor activity slips, it can affect successor activities, and consequently derails the whole project.

d. Threats

Management of IT infrastructure has to be done with diligence and requires a high level of agility and competence from relevant managers. The common threat to management of federal government IT is the lack of a thorough assessment before the implementation process. Past GAO study revealed that DON officials issued its request for proposals without a formal analysis of program alternatives to determine an appropriate acquisition strategy for NCMI, a management plan for NMCI, the funding source, and its expected effect on the existing information technology environment (Defense Acquisitions Observations, 2000). More recently, with the transition and implementation of NGEN, DON officials have failed to perform a thorough analysis to help identify the most promising acquisition approach by comparing alternative solutions' costs and operational effectiveness (GAO, 2012a).

In complex implementations such as the NGEN undertaking, there is no substitute for a healthy assessment of the current state of the organization because it defines what needs changing within the organization and what needs to remain status quo ante (Beckhard and Harris, 1987). A diligent AoA would have encompassed traditional analysis to determine a system solution based on data of a comparable system such as NMCI. The available data for NMCI were either proprietary (owned by Deloitte Consulting) or available at an aggregate level, so the PM and IPT had to rely on subject-matter experts and other sources to estimate numbers for the analysis.

To be effective, the analysis of alternatives typically includes discussions of interoperability and commonality of system elements within DoD and its agency programs. This raises the question of how the DON can assure decision makers of success with the notion of segmentation without an effective analysis. The fact is that DON cannot guarantee success based on its track record of implementing NMCI. The lack of an analysis led to cost and schedule overruns, and today the NMCI costs about $1.2 billion a year to run, with an additional $1.5 billion to run existing legacy networks (Taylor, 2008). NMCI was supposed to consolidate or eliminate disparate networks, but instead it was loosely coupled with legacy systems using middleware,[28] which still poses management problems. With the notion of segmentation, the risks are seemingly greater, especially since the relationships among segments providers and an agreement on the limits of each provider's functions has not been made (GAO, 2012a). Figure 10 is a depiction of the expected number of relationships that must be managed between the segments for NGEN to be successful.

[28] Middleware is a mechanism to move information and share business logic transparently between existing applications. It should integrate differing technologies to provide interoperability.

As the number of relationships increase it becomes more difficult to manage intricate aspects of a project and with the number of interdependencies in large technology projects the risk increase exponentially. In the Wall Street Journal article (2007) Lunsford details Boeings experiences with many contractual relationships as it sought to acquire its state of the art Dreamliner by outsourcing. The Boeing outsourcing concept consisted of a team of parts suppliers in charge of designing and building major sections of the craft, which it planned to snap together at its Seattle-area factory. The Dreamliner was a novel idea in aircraft manufacturing and required specific expertise to design and build the different segment. Boeing handpicked the suppliers but the supplier's in-turn subcontracted key tasks to even-smaller companies. Though subcontracting is a common process in large and complex projects, for Boeing it meant the first product from the novel idea was a Dreamliner with missing parts. The secondary effects of outsourcing are the delays in production of aircraft, all of which have financial commitments in place.

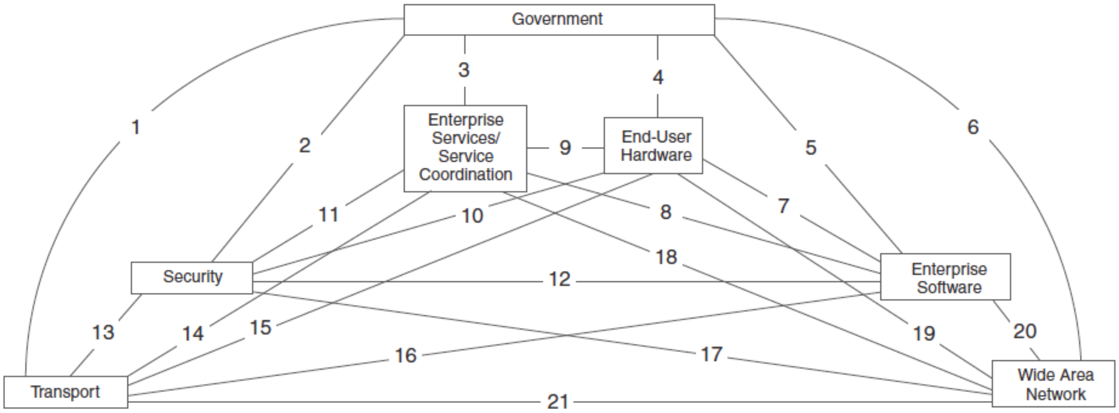


Figure 10. Contractual Relationships in Current NGEN Approach (From GAO, 2012a)

Similar to the management risk with segmentation is the management of different domains within NGEN. The threat with the division of domains is the potential to raise management concerns, especially during the formation or operation of joint commands where the possibility of the domain crossover can occur.

C. CONCLUSION

The purpose of this chapter was to illustrate how the DON and the federal government have and continue to manage IT and the effect of implementing it. Through the use of SWOT analysis the chapter contextualizes the essence of the organizational culture, its merits and disadvantages, opportunities to exploit and the risks if things remain as is. Leaders in the DoD, DON, and federal government are beginning to understand and accept cyberspace as a military domain. The current warfare environment commands a resilient and agile force that fuses the very best concepts, processes, organizations, and technology. To get to this force the U.S. must start by building the right system, on time every time. Networks serve as a conduit that connects people and their concepts, multiplying capabilities and ensuring that the U.S.'s military advantage is fully exploited.

D. ADDITIONAL RESEARCH TOPICS

This thesis has focused on the common issues that plague implementation of large IT in the DoD and the DON. It would be remiss to neglect notable mentions of the other issues that are worthy of further investigation and study. These topics are described in the subsections below.

1. Potential flaws of a Common Network

With the implementation NMCI, the DON merged over 1,000 legacy networks into a centralized and more secure network that would serve as a conduit for about 400,000 workstations and over 700,000 users across 2,500 Navy and Marine Corps locations around the world. NGEN, like NMCI, will provide data storage, e-mail, transport of voice and data, and video teleconferencing through a standardized set of hardware and software across the enterprise. This centralized network offers many advantages over isolated networks based mainly on the idea of commonality across the enterprise. Leveraging economies of scale, component reuse, sharing of common resources, and reduced development scope are a few of the benefits (Boas, 2008). The utility of commonality across the enterprise for NGEN can be immediately realized with the ability to identify and track performance metrics that can aid with decision-making such as in earned value management. The issue of concern is that with so many users that span a variety of communities of interest with varying requirements of the network, NGEN might not be flexible enough to accommodate all the requirements of the end users. A thesis in this area could explore the capabilities and limitations of NGEN, the level of "usability," and its performance in the different environments that its users will be subjected to.

2. Security

NMCI, according to GAO reports, was very secure, and with NGEN the target is a system with improved security through "continuous security assessments, a centralized distribution of vulnerability information, configuration control of critical servers, and an improved response to new vulnerabilities/threats" (GAO, 2006). NMCI had the capability to defeat over 1,200 unclassified intrusion attempts, block about nine million spam attacks and disinfect tens of thousands of viruses per month (DoD, 2009). With the acquisition approach for NGEN based on segmentation of services and potential savings, DON has to be acutely aware of the increased risk of segmentation in regard to network security. A thesis in this area could explore an effective medium of ensuring accountability among multiple contractors. One area of concern with accountability is that of IA[29] as information goes across the seams of the segmented network.

3. Cost

(1) LPTA

The risks and challenges of the low-cost technically acceptable process have been discussed in earlier sections. LPTA raises doubts about the government getting the best value, and with the imminence of more fiscal constraints in the near future; the federal government can no longer guarantee that the military is getting the best equipment available. Dependence on the LPTA is dangerous for the DoD, DON and federal agencies because, though it appears favorable as a cost saving initiative

[29] The process of protecting and defending against all forms of interference of information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation.

because of budget constraints, underbidding from contracts only guarantees a low price but does not guarantee against risk of failure. With current spending for NGEN at $1.6 billion, DON is spending over 21% of its annual budget on the implementation and associated transition activity. This expenditure raises questions of how DON can sustain the costs in the future. A thesis in this area could evaluate the impact of funding on the IT infrastructure in DoD.

(2) Navy IT Knowledge and Skills

As the battle space continually morphs to a more asymmetric front without boundaries and into global domains such as cyberspace, the government has no choice but to leverage all its parts to be successful in its mission of defending the homeland. With NGEN, the security is provided by 10th Fleet[30] and with ETA geared to strengthen the force, DON appears compliant with 8570.1M. A thesis in this area could explore how DON is and will handle limited financial resources in regard to its workforce reconstitution efforts for the implementation and management of NGEN.

E. THESIS CONCLUSION

The issues that plagued the implementation of NMCI and hinder the implementation of NGEN are not easy to address in this thesis because of the sheer level of complexity. The thesis identified some of the factors that influence the direction in which large projects like NMCI and NGEN can go, and how to militate the negative influences while leveraging the positive. Understanding these factors and the degree of influence can make the difference between failure and success of the project.

The takeaway from the thesis is the importance of doing the right thing, the right way, the first time. In both implementations, DON officials did a desultory initial assessment of the current state before implementation, and in both cases the consequences were devastating and costly. The thesis does not suggest prior analysis as a panacea for the disconcerted environment associated with IT implementation, but that a

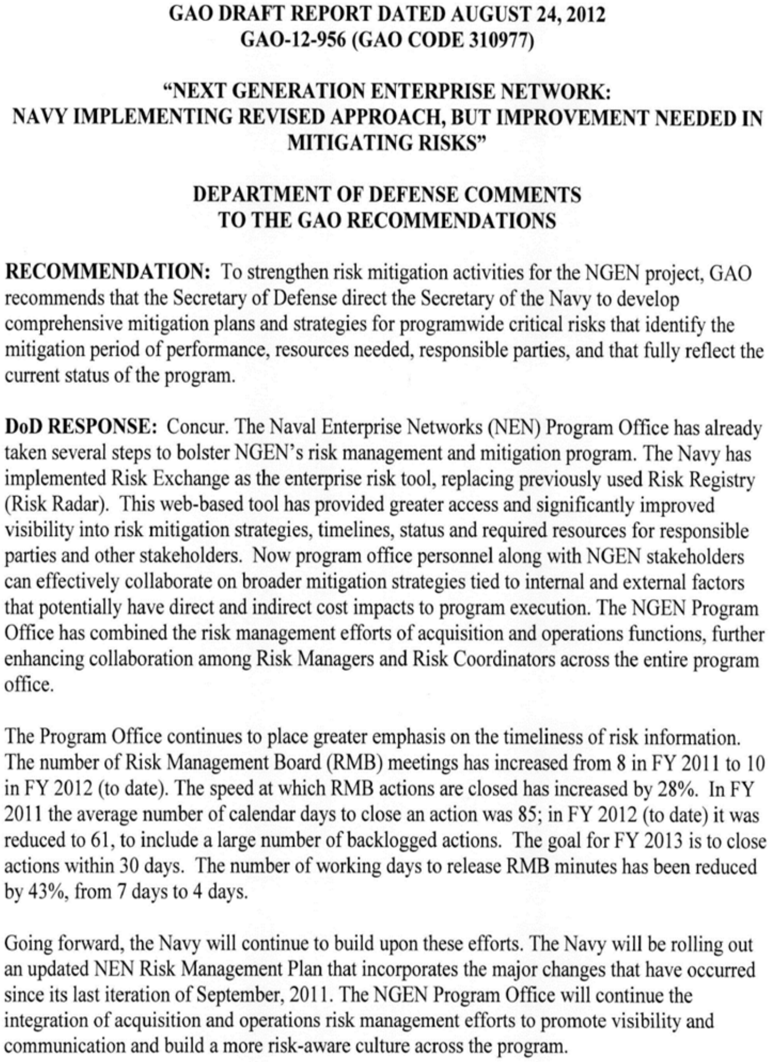
[30] U.S. Fleet Cyber Command/U.S. 10th Fleet is a functional formation of the United States Navy responsible for the Navy’s cyber warfare.

prior analysis would provide (1) information to determine if there was a real need for change, (2) a clear vision of what in the organization needs changing and what needs to remain the same, and (3) a definition the future state of the organization. The more thorough this assessment, the better the road map and the revelation of the amount of work required getting to the future state.

Finally, individuals cannot execute complex change in a large diverse organization and succeed; all stakeholders have to be a part of the solution or the project will fail. Collaboration has to be enforced at all levels of the project to ensure all relevant stakeholders buy-in the solution because people are motivated to coalesce and achieve a desired vision when there is a sense of ownership.

APPENDIX

A. DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS



GAO DRAFT REPORT DATED AUGUST 24, 2012
GAO-12-956 (GAO CODE 310977)

"NEXT GENERATION ENTERPRISE NETWORK:
NAVY IMPLEMENTING REVISED APPROACH, BUT IMPROVEMENT NEEDED IN MITIGATING RISKS"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION: To strengthen risk mitigation activities for the NGEN project, GAO recommends that the Secretary of Defense direct the Secretary of the Navy to develop comprehensive mitigation plans and strategies for programwide critical risks that identify the mitigation period of performance, resources needed, responsible parties, and that fully reflect the current status of the program.

DoD RESPONSE: Concur. The Naval Enterprise Networks (NEN) Program Office has already taken several steps to bolster NGEN's risk management and mitigation program. The Navy has implemented Risk Exchange as the enterprise risk tool, replacing previously used Risk Registry (Risk Radar). This web-based tool has provided greater access and significantly improved visibility into risk mitigation strategies, timelines, status and required resources for responsible parties and other stakeholders. Now program office personnel along with NGEN stakeholders can effectively collaborate on broader mitigation strategies tied to internal and external factors that potentially have direct and indirect cost impacts to program execution. The NGEN Program Office has combined the risk management efforts of acquisition and operations functions, further enhancing collaboration among Risk Managers and Risk Coordinators across the entire program office.

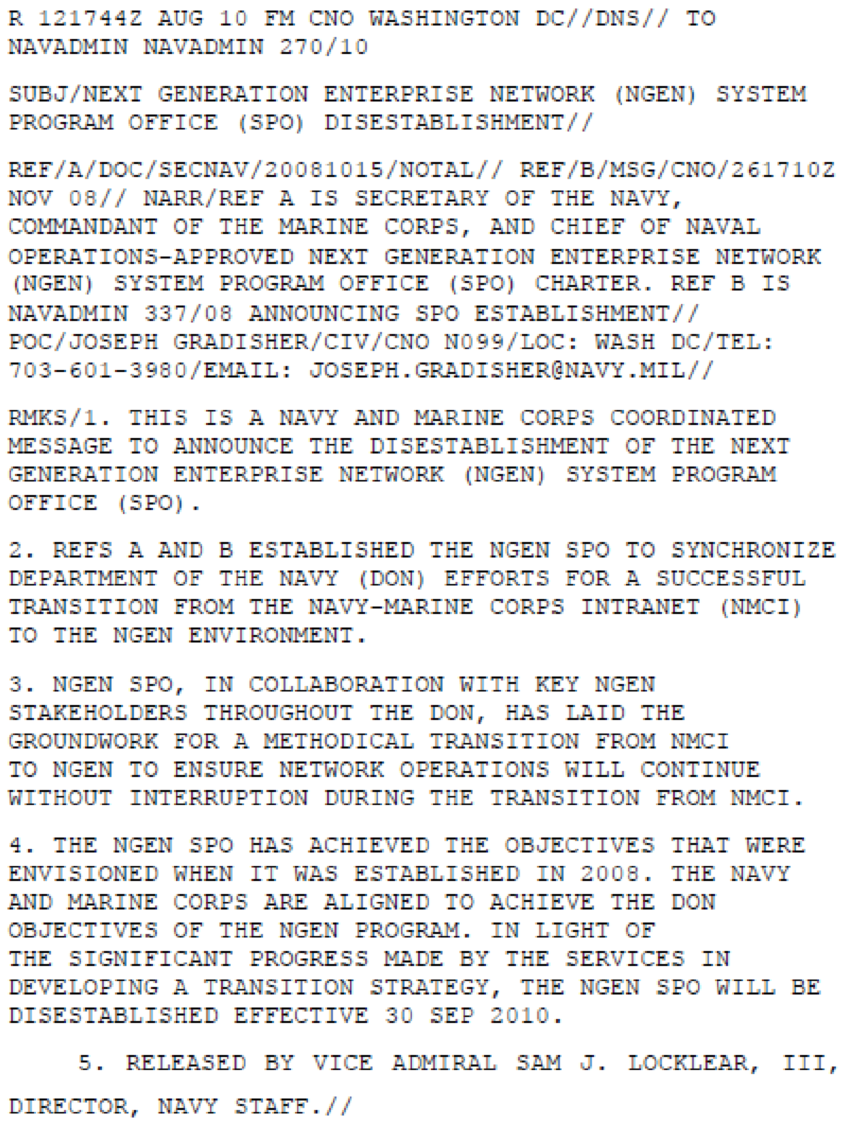
The Program Office continues to place greater emphasis on the timeliness of risk information. The number of Risk Management Board (RMB) meetings has increased from 8 in FY 2011 to 10 in FY 2012 (to date). The speed at which RMB actions are closed has increased by 28%. In FY 2011 the average number of calendar days to close an action was 85; in FY 2012 (to date) it was reduced to 61, to include a large number of backlogged actions. The goal for FY 2013 is to close actions within 30 days. The number of working days to release RMB minutes has been reduced by 43%, from 7 days to 4 days.

Going forward, the Navy will continue to build upon these efforts. The Navy will be rolling out an updated NEN Risk Management Plan that incorporates the major changes that have occurred since its last iteration of September, 2011. The NGEN Program Office will continue the integration of acquisition and operations risk management efforts to promote visibility and communication and build a more risk-aware culture across the program.

B. NAVADMIN 337/08 – NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE (SPO) ESTABLISHMENT

RTTUZYUW RUEWMCS0000 3311710-UUUU—RUCRNAD ZNR UUUUU
R 261710Z NOV 08
FM CNO WASHINGTON DC//DNS//
TO NAVADMIN
ASSTSECNAV FM WASHINGTON DC//FMB//CMC WASHINGTON DC//C4//
PEO EIS WASHINGTON DC//PEO C4I SAN DIEGO CA
COMMARCORSYSCOM QUANTICO VA
SECDEF WASHINGTON DC//NII//JOINT STAFF WASHINGTON DC//J6//
JTF-GNO WASHINGTON DC//HQ USPACOM J6COMMARFORCOM G6//
COMMARFORPAC G6//COMMARFOREUR G6//COMUSMARCENT G6//
COMMARFORK G6//DISA WASHINGTON DC//MCOTEA QUANTICO VA
MCTSSA CAMP PENDLETON CA//MCNOSC QUANTICO VA
BT
UNCLAS //N02011//
NAVADMIN 337/08
MSGID/GENADMIN/CNO WASHINGTON DC/DNS/NOV//
SUBJ/NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE
(SPO) ESTABLISHMENT//
REF/A/DOC/SECNAV/20081015/NOTAL// REF/B/DOC/CNO/20081017/NOTAL//
NARR/REF A IS SECNAV, CMC, AND CNO APPROVED NGEN SPO CHARTER. REF B IS
CNO INTERIM APPOINTMENT OF DIRECTOR NGEN SPO.// POC/MATTHEW
GHEN/LCDR/CNO N6N/LOC: WASH DC/TEL: 703-604-8388
/EMAIL: MATTHEW.GHEN@NAVY.MIL//
POC/GREG MOORE/LTCOL/HQMC C4/LOC: WASH DC/TEL: 703-693-3476
/EMAIL: GREGORY.J.MOORE@USMC.MIL//
RMKS/1. THIS IS A NAVY AND MARINE CORPS COORDINATED MESSAGE TO ANNOUNCE THE
ESTABLISHMENT OF THE NGEN SPO.
2. THE SECRETARY OF THE NAVY, CHIEF OF NAVAL OPERATIONS, AND THE
COMMANDANT OF THE MARINE CORPS HAVE COLLABORATED TO CREATE THE NGEN SPO,
UNDER THE DIRECTION OF AN ASSISTANT CHIEF OF NAVAL OPERATIONS(ACNO) REPORTING
TO NAVY AND MARINE CORPS SERVICE CHIEFS. PER REF A, THE DIRECTOR NGEN SPO WILL
BE A FLAG OFFICER WITH A USMC O6 DEPUTY. PER REF B, RDML DAVID SIMPSON HAS BEEN
DESIGNATED AS INTERIM DIRECTOR, NGEN SPO; RADM JOHN GOODWIN WILL REPORT AS
DIRECTOR IN MARCH 2009. COLONEL DAVID HAGOPIAN IS THE DEPUTY DIRECTOR.
3. REF A DESCRIBES THE MISSION, AUTHORITY, RESPONSIBILITIES, AND
ORGANIZATIONAL RELATIONSHIPS THE NGEN SPO WILL HAVE WITHIN DON FOR
GUIDING DON ELEMENTS AND SERVICES TO MISSION ACCOMPLISHMENT. THE NGEN
SPO SHALL SYNCHRONIZE THE NGEN IMPLEMENTATION WITH PRE- EXISTING
NETWORK OPERATIONS TO ENSURE CONTINUITY OF OPERATIONS THROUGHOUT THE
TRANSITION. THE NGEN SPO SHALL ENSURE THAT, UNTIL SUCCESSFUL TRANSITION
TO THE NGEN ENVIRONMENT, APPROPRIATE RISK MITIGATION STRATEGIES ARE
EMPLOYED TO ENSURE OPERATIONAL VIABILITY OF AFFECTED SERVICE NETWORKS.
IN ADDITION, THE NGEN SPO WILL WORK WITH THE RESOURCE SPONSORS TO
RECONCILE AND PRIORITIZE COMPETING REQUIREMENTS WITHIN ESTABLISHED DON
FISCAL CONSTRAINTS. THE NGEN SPO WILL ESTABLISH PROGRAM PRIORITIES, DEVELOP
PROGRAM INPUTS, EXECUTE THE NGEN PROGRAM MANAGEMENT BUDGET AND
SYNCHRONIZE ACQUISITION, OPERATIONS, SECURITY, AND TRANSITION FUNCTIONS
IN CONJUNCTION WITH THE SERVICES TO ENSURE PROGRAM WHOLENESS. THE
DURATION OF THE NGEN SPO STRUCTURE DEPENDS ON THE NEEDS OF THE SERVICES;
IT IS INTENDED THAT THE NGEN SPO SHALL EXIST THROUGH TRANSITION AT
WHICH POINT THE SERVICES MAY REEVALUATE THEIR PARTICIPATION AND SUPPORT
OF THE NGEN SPO.
4. TO EXECUTE THE MISSION ASSIGNED IN REF A, THE NGEN SPO CONSISTS OF
THREE DIVISIONS:
A. NGEN SPO ACQUISITION DIVISION (PM NGEN, PM NMCI, PM ONENET) B. NGEN SPO
OPERATIONS DIVISION C. NGEN SPO PROGRAMMING, PLANNING, AND POLICY DIVISION
5. ACTION. REF A REQUIRES DIRECTOR, NGEN SPO TO CREATE AN IMPLEMENTING DIRECTIVE
WITHIN 45 DAYS OF SPO STANDUP. NGEN SPO WILL STAFF THE INITIAL VERSION OF THE
IMPLEMENTING DIRECTIVE FOR REVIEW NO LATER THAN 1 DECEMBER. I ENCOURAGE
YOUR TEAM TO ACTIVELY PARTICIPATE IN THIS REVIEW PROCESS TO ADEQUATELY CAPTURE
ALL NGEN EQUITIES.
6. RELEASED BY VICE ADMIRAL J. C. HARVEY, JR., DIRECTOR, NAVY STAFF.//
BT
#0000
NNNN

C. NAVADMIN 270/10 – NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE (SPO) DISESTABLISHMENT



R 121744Z AUG 10 FM CNO WASHINGTON DC//DNS// TO
NAVADMIN NAVADMIN 270/10

SUBJ/NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE (SPO) DISESTABLISHMENT//

REF/A/DOC/SECNAV/20081015/NOTAL// REF/B/MSG/CNO/261710Z NOV 08// NARR/REF A IS SECRETARY OF THE NAVY, COMMANDANT OF THE MARINE CORPS, AND CHIEF OF NAVAL OPERATIONS-APPROVED NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE (SPO) CHARTER. REF B IS NAVADMIN 337/08 ANNOUNCING SPO ESTABLISHMENT// POC/JOSEPH GRADISHER/CIV/CNO N099/LOC: WASH DC/TEL: 703-601-3980/EMAIL: JOSEPH.GRADISHER@NAVY.MIL//

RMKS/1. THIS IS A NAVY AND MARINE CORPS COORDINATED MESSAGE TO ANNOUNCE THE DISESTABLISHMENT OF THE NEXT GENERATION ENTERPRISE NETWORK (NGEN) SYSTEM PROGRAM OFFICE (SPO).

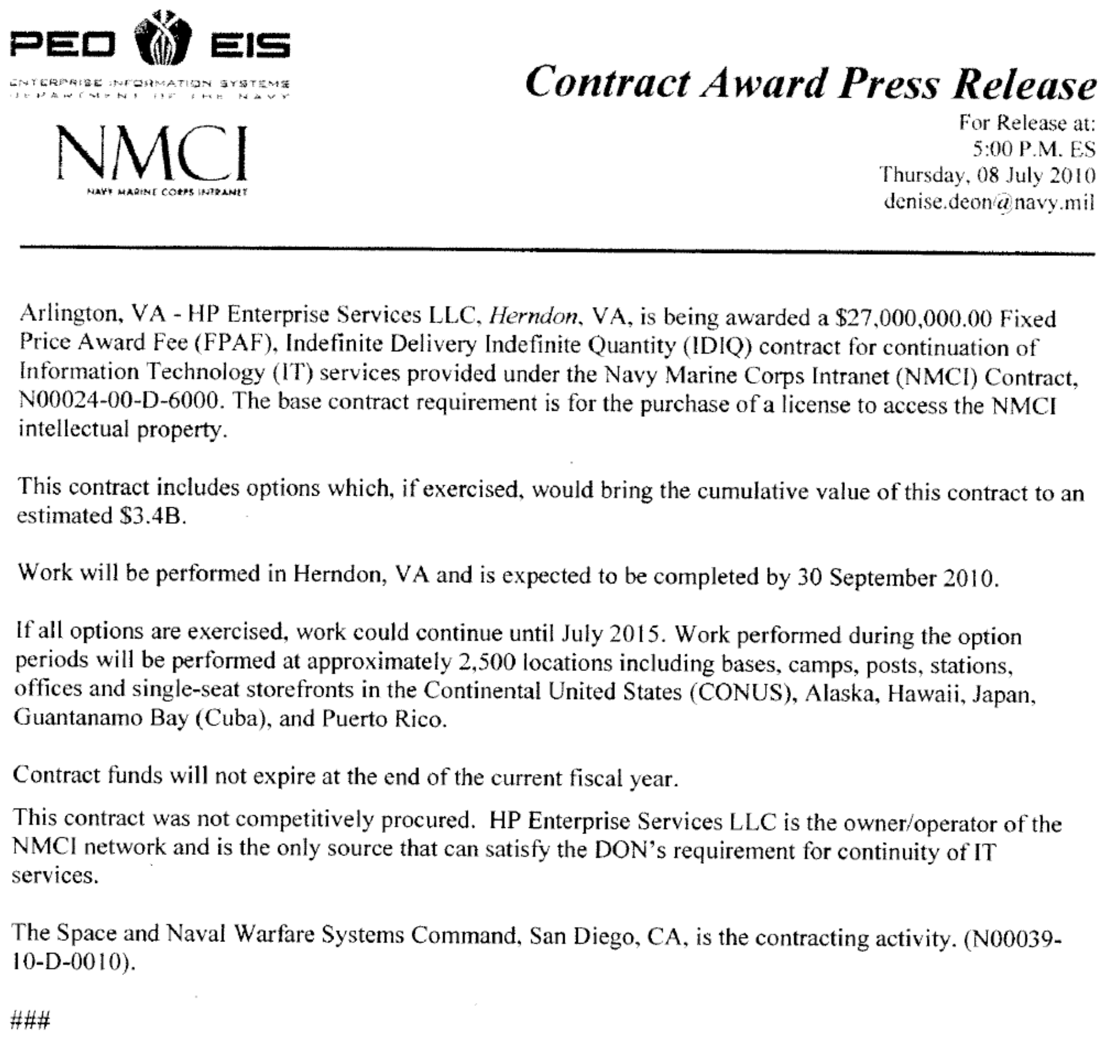
2. REFS A AND B ESTABLISHED THE NGEN SPO TO SYNCHRONIZE DEPARTMENT OF THE NAVY (DON) EFFORTS FOR A SUCCESSFUL TRANSITION FROM THE NAVY-MARINE CORPS INTRANET (NMCI) TO THE NGEN ENVIRONMENT.

3. NGEN SPO, IN COLLABORATION WITH KEY NGEN STAKEHOLDERS THROUGHOUT THE DON, HAS LAID THE GROUNDWORK FOR A METHODICAL TRANSITION FROM NMCI TO NGEN TO ENSURE NETWORK OPERATIONS WILL CONTINUE WITHOUT INTERRUPTION DURING THE TRANSITION FROM NMCI.

4. THE NGEN SPO HAS ACHIEVED THE OBJECTIVES THAT WERE ENVISIONED WHEN IT WAS ESTABLISHED IN 2008. THE NAVY AND MARINE CORPS ARE ALIGNED TO ACHIEVE THE DON OBJECTIVES OF THE NGEN PROGRAM. IN LIGHT OF THE SIGNIFICANT PROGRESS MADE BY THE SERVICES IN DEVELOPING A TRANSITION STRATEGY, THE NGEN SPO WILL BE DISESTABLISHED EFFECTIVE 30 SEP 2010.

5. RELEASED BY VICE ADMIRAL SAM J. LOCKLEAR, III, DIRECTOR, NAVY STAFF.//

D. NMCI CONTINUITY OF SERVICES CONTRACT (COSC)



PEO EIS

ENTERPRISE INFORMATION SYSTEMS
DEPARTMENT OF THE NAVY

NMCI

NAVY MARINE CORPS INTRANET

Contract Award Press Release

For Release at:
5:00 P.M. ES
Thursday, 08 July 2010
denise.deon@navy.mil

Arlington, VA - HP Enterprise Services LLC, *Herndon*, VA, is being awarded a $27,000,000.00 Fixed Price Award Fee (FPAF), Indefinite Delivery Indefinite Quantity (IDIQ) contract for continuation of Information Technology (IT) services provided under the Navy Marine Corps Intranet (NMCI) Contract, N00024-00-D-6000. The base contract requirement is for the purchase of a license to access the NMCI intellectual property.

This contract includes options which, if exercised, would bring the cumulative value of this contract to an estimated $3.4B.

Work will be performed in Herndon, VA and is expected to be completed by 30 September 2010.

If all options are exercised, work could continue until July 2015. Work performed during the option periods will be performed at approximately 2,500 locations including bases, camps, posts, stations, offices and single-seat storefronts in the Continental United States (CONUS), Alaska, Hawaii, Japan, Guantanamo Bay (Cuba), and Puerto Rico.

Contract funds will not expire at the end of the current fiscal year.

This contract was not competitively procured. HP Enterprise Services LLC is the owner/operator of the NMCI network and is the only source that can satisfy the DON's requirement for continuity of IT services.

The Space and Naval Warfare Systems Command, San Diego, CA, is the contracting activity. (N00039-10-D-0010).

###

LIST OF REFERENCES

Addy, R. (2010). *Effective IT service management: to ITIL and beyond!* Berlin: Springer.

Anderson, D., & Anderson, L. S. (2001). *Beyond change management advanced strategies for today's transformational leaders*. San Francisco: Jossey-Bass/Pfeiffer.

Baccarini, D., Salm, G., & Love, P.E.D. (2004). “Management of risks in information technology projects,” *Industrial Management & Data Systems*, *104*(4), 286–295. Retrieved from http://dx.doi.org/10.1108/02635570410530702

Beckhard, R., & Harris, R. T. (1987). *Organizational transitions: Managing complex change*, 2nd ed. Reading, MA.: AddisonWesley Publishing.

Beer, M. (1980). *Organization change and development: a systems view*. Santa Monica, CA: Goodyear Publishing.

Benamati, J., Lederer, A. L., & Singh, M. (1998). Information technology change: The impact on it management. *Journal of Computer Information Systems*, *38*(4), 9–13. Retrieved from http://search.proquest.com/docview/232578782?accountid=12702

Bennatan, E. M. (2000). *On time within budget: software project management practices and techniques*,3rd ed. New York, NY: Wiley.

Bishnoi, R. (2006, June 6). Navy, Marine Corps mull standards for successor to NMCI. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-06/26/2006/navy-marine-corps-mull-standards-for-successor-to-nmci/menu-id-150.html

Boas, R. (2008). *Commonality in complex product families: Implications of divergence and lifecycle offsets.*(Doctoral dissertation). Massachusetts Institute of Technology, Cambridge, MA. Retrieved from http://hdl.hanle.net/1721.1/53209

Bridges, W. (2009). *Managing transitions: making the most of change*, 3rd ed. Philadelphia, PA: Da Capo Lifelong.

Brynjolfsson, E., Renshaw, A. A. , & Alstyne, M. (1997, January 15). The Matrix of Change: A Tool for Business Process Reengineering. *Sloan Management Review*, 37–54.

Bryson, J.M. (2004). What to do when stakeholders matter: Stakeholder identification analysis techniques. *Public Management Review*, *6*(1), 21–53. doi: 10.1080/14719030410001675722

Burt, A. (2010). Weaning NMCI off HP 300 Personnel To Oversee NMCI As Navy Takes More Control. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-09/06/2010/300-personnel-to-oversee-nmci-as-navy-takes-more-control/menu-id-150.html

Castelli, C. (2010, February 25). DoD Kick-Starts Development Of Successor To World's Largest Intranet. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Pentagon/Inside-the-Pentagon-02/25/2010/dod-kick-starts-development-of-successor-to-worlds-largest-intranet/menu-id-148.html

Cervone, F. (2008). *ITIL: a framework for managing digital library services*, OCLC Systems & Services, *24*(2), 87–90

CHIPS Magazine.(2009, January–March). Top 10 Questions about NGEN with answers from DON CIO Rob Carey. *Chips Magazine*. Retrieved from http://www.DONcio.Navy.mil/CHIPS/ArticleDetails.aspx?ID=2698

CHIPS Magazine. (2010, January–March). Getting from NMCI to NGEN, early transition activities will ensure the seamless follow-on of the Next Generation Enterprise Network. *Tim Holland*. Retrieved from http://www.DONcio.Navy.mil/CHIPS/ArticleDetails.aspx?ID=2558

Clinger-Cohen Act of 1996, Pub. L. No. 104-106, 110 Stat. 186 (1996), codified at 40 U.S.C §11101 et seq .

Cunningham, M. (1999). It’s all about the business. *Information & Management, 13* (3), 83.

Defense Acquisition University (DAU), (n.d.). [Fact sheet]. Retrieved from http://www.dau.mil/default.aspx

Defense Daily Network (DDN). (2008). *Defense Industry news, analysis and business information*, *239*(65). Retrieved from http://www.defensedaily.com/index.html

Department of Defense (DoD). (1998). Levels of Information Systems Interoperability (LISI). Retrieved from http://www.eng.auburn.edu/~hamilton/security/DoDAF/LISI.pdf

Department of Defense (DoD). (2009). *Final Report on Defense Business Operations to the Congressional Defense Committees*. Washington DC: Office of Congressional Information and Publishing. Retrieved from http://dcmo.defense.gov/publications/documents/March_2009_Congressional_Report%20.pdf

Department of Defense appropriations bill, 2012 report (to accompany H.R. 2219). (2011). Washington, DC: U.S. G.P.O.

Department of Defense DIRECTIVE 8570.1-M (1990). Clinical training in serious mental illness (DHHS Publication No. ADM 90-1679). Washington, DC: U.S. Government Printing Office.

Department of the Navy. (2008a). *Next Generation Enterprise Network (NGEN) Requirements Document.* Washington, DC: NGEN Requirements Task Force.

Department of the Navy. (2008b). *Next Generation Enterprise Network: Network Operations (NetOps) Concept of Operations (CONOPS).* Washington, DC:

Department of the Navy. (2009). *Continuity of Services Contract (CoSC) Solicitation Number: N00039-09-R0052*. Retrieved from https://www.fbo.gov/?s=opportunity&mode=form&id=ec681a1f067af453267ab120ebf877cb&tab=core&cview=1

Department of the Navy. (2012). *Next Generation Enterprise Network (NGEN) Final RFP Solicitation Number: N00039-09-R0052*. Retrieved from https://www.fbo.gov/?s=opportunity&mode=form&id=ec681a1f067af453267ab120ebf877cb&tab=core&cview=1

Department of the Navy, Enterprise Licensing Agreements (DON ELA) (2012) *Mandatory use of Department of the Navy Enterprise Licensing Agreements*. Washington, DC Retrieved from http://www.doncio.navy.mil/uploads/0224ZJX12672.pdf

Department of the Navy Naval Networking Environment (NNE)-2016. (2008). *Strategic Definition, Scope and Strategy Paper, Version 1.1. (132008).* Ft. Belvoir: Defense Technical Information Center. Retrieved from http://www.doncio.navy.mil/uploads/0514WIJ91142.pdf

Director, Operational test and Evaluation (DOT&E). (2003). FY-2003 Annual Report *Office of the Director, Operational Test & Evaluation.* Retrieved from http://www.dote.osd.mil/pub/reports/FY2003/

Engming, L., & Hsieh, C. T. (1994). Seven deadly risk factors of software development projects. *Journal of Systems Management*, *36*(6), 38 – 42.

Federal Acquisition Regulations, 15.203 (FAR, 2003, § 15.203) *Requests for proposals.* Retrieved from http://www.gpo.gov/fdsys/pkg/CFR-2003-title48-vol1/pdf/CFR-2003-title48-vol1-sec15-203.pdf

Freeman, R. E. (1984). Strategic management: A stakeholder approach. Boston: Pitman, Fuerst, W.L. and Cheney, P.H. (1982). Factors affecting the perceived utilization of computer based decision support systems in the oil industry. *Decision Sciences, 13*(3), 44–69. doi: 10.1111/j.15405915.1982.tb01182.x

Gardner, J., (1987). Leaders and Followers, *Liberal Education 73*(2), 46.

Gibson, C. F. (2004). IT-enabled business change: An approach to understanding and managing risk. *MIS Quarterly Executive 2*(2), 104–115.

Gillam, M., (2010). *Exploring the impact of the clinger-Cohen act on information technology governance: A phenomenological study. Dissertation Abstracts International, B: Sciences and Engineering*, 2660 – 2660. Retrieved from http://search.proquest.com/docview/818820229?accountid=12702.

Global IT project management survey / KPMG Information Risk Management group. (2005). Sydney, Australia: KPMG.

Goss,T., Pascale, R. & Athos, A. (1998). The reinvention roller coaster: risking the present for a powerful future. *Harvard business review on change.* Boston, MA: Harvard Business School Publishing.

Government Accountability Office (GAO). (1991, November). *Government Contractors: Are Service Contractors Performing Inherently Governmental Functions? Report to the Chairman, Federal Service, Post Office and Civil Service Subcommittee, Committee on Governmental Affairs* (GAO/GGD9211) Retrieved from http://archive.gao.gov/t2pbat7/145453.pdf

Government Accountability Office (GAO) (1998, March). *Accounting and Information Management Division; Executive guide measuring performance and demonstrating results of information technology* investments (GAO/AIMD–98–89). Washington, DC: U.S. General Accountability Office. Retrieved from http://www.gao.gov/assets/80/76378.pdf

Government Accountability Office (GAO). (1998, June). *Report to House of Representatives Committee on National Security: DoD's information assurance efforts* (GAO/NSIAD-98-132R). Washington, DC U.S. General Accounting Office. Retrieved from http://www.gao.gov/assets/90/87860.pdf

Government Accountability Office (GAO). (2000, March). *Defense Acquisitions; Observations on the Procurement of the Navy/Marine Corps Intranet. Testimony Before the Subcommittees on Military Readiness and Military Research and Development, Committee on Armed Services, House of Representatives* (GAO/T-NSIAD/AIMD-00-116). Washington, DC U.S. General Accounting Office. Retrieved from http://www.gao.gov/assets/90/81621.pdf

Government Accountability Office (GAO). (2003, April). *Information technology; DoD needs to leverage lessons learned from its outsourcing projects: Report to the Subcommittee on Readiness and Management Support, Committee on Armed Services, U.S. Senate* (GAO-03-371). Washington, DC: United States General Accounting Office. Retrieved from http://www.gao.gov/products/GAO-03-371

Government Accountability Office (GAO). (2004, March). *Information technology investment management; a framework for assessing and improving process maturity: executive guide* (GAO-04-394G). Washington, DC: U.S. General Accountability Office. Retrieved from http://www.gao.gov/assets/80/76790.pdf

Government Accountability Office (GAO). (2006, December). *Information technology; DoD needs to ensure that Navy Marine Corps Intranet program is meeting goals and satisfying customers: report to congressional addressees* (GAO-07-51). Washington, DC U.S. General Accounting Office. Retrieved from http://www.gao.gov/assets/260/254360.pdf

Government Accountability Office (GAO) (2008a, October). *Information technology; management improvements needed on the Department of Homeland Security's Next Generation Information Sharing System: report to congressional requesters* (GAO-09-40). Washington, DC: U.S. General Accountability Office. Retrieved from http://www.gao.gov/assets/290/282633.pdf

Government Accountability Office (GAO). (2008b, July). *Information technology; OMB and agencies need to improve planning, management, and oversight of projects totaling billions of dollars: testimony before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and Intern* (GAO-08-1051T). Washington, DC: Government Accountability Office. Retrieved from 2012, http://www.gao.gov/assets/130/120968.pdf

Government Accountability Office (GAO). (2008c, July). *Information technology agencies need to establish comprehensive policies to address changes to projects' cost, schedule, and performance goals: report to congressional requesters* (GAO-08-925). Washington, DC: Government Accountability Office. Retrieved from http://www.gao.gov/new.items/d08925.pdf

Government Accountability Office (GAO). (2009). *Cost Estimating and Assessment Guide - Best Practices for Developing and Managing Capital Program Costs* (GAO-09-3SP). S.l.: Washington, DC U.S. General Accounting Office. Retrieved from http://www.gao.gov/assets/80/77175.pdf

Government Accountability Office (GAO). (2010a, October). *DoD business transformation improved management oversight of business system modernization efforts needed: Report to congressional requesters* (GAO-11-53). Washington, DC: U.S. Govt. Accountability Office. Retrieved from http://www.gao.gov/new.items/d1153.pdf

Government Accountability Office (GAO). (2010b, June). *Report to Subcommittee on Commerce, Justice, Science, and Related Agencies Response to addresses the Government Accountability Office's (GAO) access to information*. (B-319956).Washington, DC U.S. General Accounting Office. Retrieved from http://www.fas.org/sgp/gao/access.pdf

Government Accountability Office (GAO). (2011a, March). *Information Technology: Better Informed Decision Making Needed on Navy's Next Generation Enterprise Network Acquisition* (GAO-11-150). Washington, DC U.S. General Accounting Office. Retrieved from http://www.gao.gov/new.items/d11150.pdf

Government Accountability Office (GAO). (2011b, October). *Information technology critical factors underlying successful major acquisitions: report to congressional committees* (GAO-12-7). Washington, DC: U.S. Govt. Accountability Office. Retrieved from http://www.gao.gov/new.items/d127.pdf

Government Accountability Office (GAO). (2012a, September). *Next Generation Enterprise Network: Navy implementing revised approach, but improvement needed in mitigating risks: report to congressional requesters* (GAO-12-956). Washington, DC: U.S. Govt. Accountability Office. Retrieved from http://www.gao.gov/assets/650/648566.pdf

Government Accountability Office (GAO). (2012b, April). *Information technology reform progress made; more needs to be done to complete actions and measure results: report to congressional requesters* (GAO-12-461). Washington, DC: U.S. Govt. Accountability Office. Retrieved from http://www.gao.gov/assets/600/590457.pdf

Wooldridge, M.B., & Shapka, J. (2012). Playing with technology: Mother-toddler interaction scores lower during play with electronic toys. *Journal of Applied Developmental Psychology*, *33*(5), 211 – 218. http://dx.doi.org/10.1016/j.appdev.2012.05.005

Gutierrez, O., & Friedman, D., (2005). Managing projects expectations in human services information systems implementations: The case of homeless management information systems. *International Journal of Project Management*, *23*(7), 513 – 523. http://dx.doi.org/10.1016/j.ijproman.2005.02.006

Hannon, T. (2004). *An External Stakeholder Analysis of a United States Army Directorate of Contracting* (Masters thesis, Naval Postgraduate School) Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2004/Dec/04Dec_Hannon.pdf

Hodges, J., (2011) Course correction; U.S. Navy simplifies acquisition plan for next intranet amid storm of complaints,*C4ISR10*(9). Retrieved from http://www.dtic.mil/dtic/aulimp/citations/gsa/2011190183/190016.html

Holland, T. (2010) *Next Generation Enterprise Network (NGEN); NGEN Acquisition Industry Day Brief* [Presentaton slides]. Retrieved from http://www.public.navy.mil/spawar/PEOEIS/NEN/NGEN/Documents/Industry_Day_Slides_28_OCT_2011_FINAL_DISTA_10312011_S.pdf

Hudson, L. (2011, December 19). NGEN will not face any 'anticipated' schedule or integration delays. *InsideDefense.com.* Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-12/19/2011/ngen-will-not-face-any-anticipated-schedule-or-integration-delays/menu-id-150.html

Hudson, L. (2012, August 9). Navy: NGEN delays caused $2.1 billion boost in NMCI price ceiling. *InsideDefense.com.* Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Pentagon/Inside-the-Pentagon-08/09/2012/navy-ngen-delays-caused-21-billion-boost-in-nmci-price-ceiling/menu-id-148.html

Hudson, L. (2012, January 16). Final RFP this month; competition widens for the next generation Enterprise Network. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-01/16/2012/competition-widens-for-the-next-generation-enterprise-network/menu-id-150.html

Information Technology Infrastructure Library (ITIL). (n.d.). The Information technology infrastructure library for the IT service management organization. [Fact sheet] Retrieved from http://www.itilofficialsite.com/AboutITIL/WhatisITIL.aspx

Jordan, K., & Johnson, S. (2007, September). *The NMCI experience and lessons learned: the consolidation of networks by outsourcing*. Retrieved from National Defense University website: http://www.ndu.edu/CTNSP/docUploaded/Case%2012%20%20The%20NMCI%20Experience%20and%20Lessons%20Learned.pdf

Kanter, R. M., Stein, B., & Jick, T. (1992). *The Challenge of organizational change: How companies experience it and leaders guide it*. New York, NY: Free Press.

Kundra, V. (2010). *25-point implementation plan to reform federal information technology management*. Washington DC: The White House, Chief Information Officers Council.

Long, S., & Spurlock, D. G. (2008). Motivation and Stakeholder Acceptance in Technology-driven Change Management: Implications for the Engineering Manager. *Engineering Management Journal*, 20(2), 30 – 36. Retrieved from https://login.libproxy.newschool.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=35343988&site=ehost-live&scope=site

Lunsford, L. (2007, December 7). Jet Blues; Boeing Scrambles to Repair Problems With New Plane. *The Wall Street Journal Online*. Retrieved from http://online.wsj.com/article_print/SB119698754167616531.html

Ma, J. (2003, August 25). Worm hits 75 percent of NMCI workstations, but most are now clear. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-08/25/2003/worm-hits-75-percent-of-nmci-workstations-but-most-are-now-clear/menu-id-150.html

Ma, J. (2003, December 22). Facing delays, completion of NMCI roll out now expected next year. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-12/22/2003/facing-delays-completion-of-nmci-roll-out-now-expected-next-year/menu-id-150.html

Ma, J. (2004). Inside the Navy; incentives offer potential windfalls for EDS in money-losing NMCI. *InsideDefense.com*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-09/06/2004/incentives-offer-potential-windfalls-for-eds-in-money-losing-nmci/menu-id-150.html

Marine Corps Doctrinal Publications (MCDP) 6 (1996). Command and Control Washington, D.C: Dept. of the Navy.

Mitchell, R., Agle, B., & Wood, D. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review*, 22(4), 853 – 886.

Munns, C. L. (2003, January). A Global Navy Needs a Global Network. *United States Naval Institute*, *129*(1) 60–62.

Murphy, J.T. (1988). The unheroic side of leadership: Notes from the swamp [Web log Post]. Retrieved from http://www.sedl.org/change/leadership/history.html

National Institute of Standards and Technology (NIST).(2009). *NIST Special Publication Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process*. Retrieved from http://csrc.nist.gov/publications/drafts/80065rev1/draftsp80065rev1.pdf

Naval Enterprise Networks (NEN). (n.d.). U.S. Navy Hosting [Fact sheet]. Retrieved from http://www.public.Navy.mil/spawar

Onley, D.S. (2002, November 1). Bush signs $1.96 billion NMCI extension. *Government Computer News*: Retrieved from http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=474D-TG40-00G8-P4K1&csi=167445&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true

Onley, D.S. (2005, August 19). Navy to set up central office for management of IT funds *Government Computer News*: Retrieved from http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=4GXV-SVM0-00G8-P4DD&csi=167445&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true

Pasmore, W. (2011). Tipping the balance: Overcoming persistent problems in organizational change. In R. Woodman, W. Pasmore, & A. Shani (Eds.), *Research in organizational change and development, 19,* 259 – 292. Bingley, UK: Emerald Group.

Perkins, S. (2005). Navy Marine Corp Intranet (NMCI). *Babson Legislative Education*, BEE SP0805, 14.

Plummer, A. (2001, December 20). Bill outlines stringent checkpoints for Navy-marine Corps intranet. *Inside the Pentagon*. Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Pentagon/Inside-the-Pentagon-12/20/2001/bill-outlines-stringent-checkpoints-for-navy-marine-corps-intranet/menu-id-148.html

Riley, E. (2008, October 30). New governance structure for next generation enterprise network created. *The U.S. Navy*. Retrieved from http://www.Navy.mil/submit/display.asp?storyid=40601

Schneider, G. (2000, October 7). Navy Embraces Online Mission; EDS Gets $7 Billion-Dollar Intranet Job. *The Washington Post*. Retrieved from http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=41C6-GM20-00RP-M3FB&csi=8075&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true

Senge, P. M. (1990). *The fifth discipline: the art and practice of the learning organization*. New York: Doubleday/Currency.

Sergiovanni, T.J. (1990). Adding value to leadership gets extraordinary results. educational leadership. [Web log Post] Retrieved from http://www.sedl.org/change/issues/issues23.html

Service Oriented Architecture (SOA). Acquisition Working Group. (2008). *An Executive Forum on Business Change; Industry Recommendations for DoD Acquisition of Information Services and SOA Systems*. Retrieved from http://www.afei.org/WorkingGroups/IndustryAdvisoryGroupIAG/Documents/SOA-Acquisition%20Final%20ReportV4.pdf

Shalikashvili, J. M. (1997). *Joint Vision 2010: America's Military: Preparing for Tomorrow*. Ft. Belvoir, VA. Joint Chiefs of Staff.

Shand, M. (1994). User manuals as project management tools. II. Practical applications, *Professional Communication, IEEE Transactions on*, *37*(3) 12 –142. http://dx.doi.org/10.1109/47.317478

Shane, J. (2010). Performance management in police agencies: a conceptual framework, Policing: *An International Journal of Police Strategies & Management*, *(33)*1, 6–29. http://dx.doi.org/10.1108/13639511011020575

Shillabeer, A., Buss, T., & Rousseau, D. (2011). *Evidence based public management practices, issues, and prospects*. Armonk, N.Y.: M.E. Sharpe

Stanford Research Institute (2005) SRI Information Page. Retrieved from http://www.sri.com/sites/default/files/brochures/dec-05.pdf

Taylor, D., (2008, March 3). *Navy to spend $70 million this year to beef up NMCI, NGEN security. InsideDefense.com.* Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-03/03/2008/navy-to-spend-70-million-this-year-to-beef-up-nmci-ngen-security/menu-id-150.html

Taylor, D., (2010, July 19). *Stackley: Navy to spend $3.3 billion to keep nmci online into FY-14. InsideDefense.com.* Retrieved from http://insidedefense.com.libproxy.nps.edu/Inside-the-Navy/Inside-the-Navy-07/19/2010/stackley-navy-to-spend-33-billion-to-keep-nmci-online-into-fy-14/menu-id-150.html

Taylor G. (2006). *NMCI: history, implementation, and change*. (Master's thesis, Naval Postgraduate School). Retrieved from http://edocs.nps.edu/npspubs/scholarly/theses/2006/Sep/06Sep%5FTaylor.pdf

Thomsett, R. (2002). *Project Pathology, Causes, patterns and symptoms of project failure*. Retrieved from http://www.thomsett.com.au/main/articles/path/toc.htm

Two guys meet, one gets sold: thoughts and stories about the actual "world's oldest profession." (2013). [Web log post]. Retrieved from http://www.mrmcgu.com/

U.S. Constitution, Art. I, § 8

U.S. Department of Defense (DoD). (2009). Final Report on Defense Business Operations to the Congressional Defense Committees. Retrieved from http://dcmo.defense.gov/publications/documents/March2009CongressionalReport%20.pdf

United States Congress House of Representatives, Committee on Armed Services. (2011). Challenges to doing business with the Department of Defense hearing before the Panel on Business Challenges within the Defense Industry of the Committee on Armed Services, House of Representatives, One Hundred Twelfth Congress, first session, hearing held September 20, 2011. Washington: U.S. G.P.O.

United States Congress House of Representatives, Committee on Armed Services. (2012). Challenges to doing business with the Department of Defense; Findings of the Panel on Business Challenges in the Defense Industry before Committee on Armed Services, House of Representatives, hearing held March 19, 2012.. Washington, DC: Retrieved from, http://armedservices.house.gov/index.cfm/files/serve?File_id=f60b62cb-ce5d-44b7-a2aa-8b693487cd44

Umble, E. J., Haft, R., & Umble, M. (2003). Enterprise resource planning: Implementation procedures and critical success factors. *European Journal of Operational Research*, *146*(2), 241257. Retrieved from http://www.sciencedirect.com.library.capella.edu/science?

Ward, J., & Elvin, R. (1999). A new framework for managing IT enabled business change. *Information Systems Journal*, *9*(3), 197 – 221. http://dx.doi.org/10.1046/j.13652575.1999.00059.x

Westley, F. & Mintzberg, H. (1989). Visionary leadership and strategic management. *Strategic Management Journal*, *10*, 17 – 32. Retrieved from http://onlinelibrary.wiley.com/store/10.1002/smj.4250100704/asset/4250100704ftp.pdf?v=1&t=hcuvacgu&s=e6e1f887307b060dfd11074866d2560d9a985065

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Dan Boger
   Chair, Department of Information Science
   Naval Postgraduate School
   Monterey, California

4. Dr. Frank Barrett
   Professor of Management and Organizational Behavior
   Professor of Global Public Policy
   Graduate School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California

5. Dr. Mark Nissen
   Graduate School of Operational and Information Sciences
   Graduate School of Business and Public Policy
   Naval Postgraduate School
   Monterey, California